ARCHIVES OF MATHEMATICS

ARCHIV DER MATHEMATIK

ARCHIVES MATHÉMATIQUES

Begründet von W. SÜSS

Herausgegeben in Verbindung mit dem Mathematischen Forschungsinstitut in Oberwolfach

von R. BAER · H. KNESER

INHALT – CONTENTS – SOMMAIRE

ARCH. MATH.	VOL. XII	FASC. 1	PAG. 1—80	1. III. 1961

BIRKHÄUSER VERLAG · BASEL UND STUTTGART

ARCHIV DER MATHEMATIK

ARCHIVES OF MATHEMATICS — ARCHIVES MATHÉMATIQUES

Adresse der Redaktion: Würzburg (Deutschland), Klinikstraße 6

Das *Archiv der Mathematik* erscheint regelmäßig alle 2 Monate mit jährlich 6 Heften. De Bezugspreis beträgt für den ganzen Band Fr. 66.— (DM 66.—) und für das Einzelheft Fr. 14.— (DM 14.—). Mitglieder einer der nachstehend genannten Gesellschaften erhalten hierauf 20% Rabatt: *Canadian Mathematical Congress · Deutsche Mathematiker-Vereinigung · Gesellschaft fü angewandte Mathematik und Mechanik · Het Wiskundig Genootshap te Amsterdam · Indian Mathe matical Society · Matematisk Forening i Kobenhavn · Norsk Matematisk Forening · Österreichisch Mathematische Gesellschaft · Polskie Towarystwo Matematyczne · Schweizerische Mathematisch Gesellschaft · Sociedad Matemática Española · Société Mathématique de France · The America Mathematical Society · The Edinburgh Mathematical Society · The London Mathematical Society The Mathematical Association of America · Unión Matematica Argentina · Unione Matematic Italiana.*

Veröffentlicht werden in erster Linie *Originalarbeiten* aus dem Gesamtgebiet der *Mathemati* und ihrer unmittelbaren Anwendungen. In beschränktem Maße können auch *Selbstreferate* übe bislang unveröffentlichte größere Arbeiten, deren wissenschaftliche Bedeutung dies gerechtfertig erscheinen läßt, Aufnahme finden. In diesen Selbstreferaten müssen außer den Resultaten di wesentlichen Schritte der Beweisführung mitgeteilt werden. Schließlich gelangen in zwanglose Folge *Zusammenfassende Berichte* über die Fortschritte einzelner Sondergebiete, die in rasche Entwicklung begriffen sind, mit ausführlichen Literaturangaben zum Abdruck.

Die Manuskripte können in deutscher, englischer, französischer oder italienischer Sprach abgefaßt sein und sollen an Umfang 10 Druckseiten nicht überschreiten. Die Autoren werde gebeten, die Manuskripte in Maschinenschrift mit handschriftlich eingetragenen Formeln ein zureichen und ihnen separat eine «Anweisung für den Setzer» beizufügen, aus der zu ersehen ist wie kursiver, gesperrter oder fetter Satz, Kleindruck und griechische, Fraktur-, Antiqua- un sonstige Typen durch farbige Unterstreichungen kenntlich gemacht sind. Die Vorlagen für Ab bildungen müssen reproduktionsfertig und mit Reduktionsmaßstab versehen eingeliefert werden Beschriftung der Abbildung jedoch nur mit Bleistift, am besten auf einem lose vorgeklebten durchsichtigen Papier. Nicht durch die Druckerei verschuldete Autorkorrekturen, welche 10% der reinen Satzkosten übersteigen, werden den betreffenden Autoren belastet.

Eine Honorierung der Beiträge erfolgt nicht. Den Verfassern werden 75 Separata ohne Um schlag gratis überlassen; weitere Fortdrucke bzw. Umschläge für Separata, sofern ihre Bestellun bei Rückgabe der Korrektur aufgegeben wird, können gegen folgende Berechnung geliefer werden: Je 25 Fortdrucke DM 0,80 pro Seite (ohne Umschlag); erste 25 Umschläge DM 18.— je weitere 25 Umschläge DM 6.—.

Redaktionsschluß spätestens 3 Monate vor Erscheinungstermin des jeweiligen Heftes. Sämt liche *Zuschriften* sind an die obengenannte Adresse der Redaktion erbeten.

Gesamtherstellung: Konrad Triltsch, Graphischer Großbetrieb, Würzburg

---

Die Auslieferung dieser Zeitschrift erfolgt für Deutschland durch den Birkhäuser Verlag, Stuttga Olgastraße 53 und für alle übrigen Staaten durch den Birkhäuser Verlag in Basel.

Über die p-Untergruppen endlicher Gruppen

Von

Wolfgang Krull

Für den grundlegenden Sylowschen Satz: „Für jede in der Ordnung $o(G)$ der Gruppe G aufgehende Primzahlpotenz p^r ist die Anzahl Z_{G,p^r} aller Untergruppen p^r-ter Ordnung positiv" hat Herr Wielandt kürzlich einen neuen Beweis angegeben, der an Einfachheit und Eleganz nichts zu wünschen übrig läßt[1]. Im Folgenden wird gezeigt, daß durch Weiterentwicklung der Wielandtschen Grundgedanken fast ebenso einfach die schärfere Formel $Z_{G,p^r} \equiv 1\,(p)$ gewonnen werden kann. Anschließend wird untersucht, wie sich auf Grund dieser Formel die elementaren Sätze über p-Gruppen (Überauflösbarkeit der p-Gruppen, Sylowuntergruppen beliebiger endlicher Gruppen) möglichst kurz und einfach herleiten lassen. Die Formulierungen sind dabei z. T. schärfer als in den verbreiteten Lehrbüchern üblich. Im übrigen ist es ein Hauptziel der Note, die den Beweisen zugrundeliegenden Methoden in voller Allgemeinheit klar herauszuarbeiten.

Im Sinne des zweiten Programmpunkts beginnen wir mit der Formulierung von einigen Begriffsbildungen und Sätzen, die zwar nicht „elementar" im klassischen Sinne sind, aber doch so einfach und wichtig, daß sie in keinem modernen Algebralehrbuch fehlen sollten.

Es sei G eine (zunächst nicht notwendig endliche) Gruppe mit den Elementen a, $b, \ldots$; $\mathfrak{M}$ sei eine Menge mit den Elementen $A, B, \ldots$. Dann soll G *Operatorgruppe auf* $\mathfrak{M}$ heißen, wenn folgende Bedingungen erfüllt sind:

1. Jedem Paar $a \in G$, $A \in \mathfrak{M}$ ist eindeutig ein Element $B = aA$ aus $\mathfrak{M}$ zugeordnet.
2. Es gilt das assoziative Gesetz, d. h. es wird stets $a(bA) = (a \cdot b)A$.
3. G ist auf $\mathfrak{M}$ unitär, d. h. das Einselement e von G genügt der Bedingung $eA = A$ für alle $A \in \mathfrak{M}$[2].

Ist G Operatorgruppe auf $\mathfrak{M}$, so bildet für festes $A \in \mathfrak{M}$ die Menge aller $u \in G$ mit $uA = A$ eine Untergruppe F_A von G, die als *Fixgruppe von A* (*in* G) bezeichnet wird.

[1]) Vgl. H. Wielandt, Ein Beweis über die Existenz der Sylowgruppen. Arch. Math. 10, 401 bis 402 (1959).

[2]) Natürlich erzeugt jedes $a \in G$ eine Permutation π_a von $\mathfrak{M}$ (also eine umkehrbar eindeutige Abbildung von $\mathfrak{M}$ auf $\mathfrak{M}$), und die Zuordnung $a \to \pi_a$ definiert einen Homomorphismus von G in die Gruppe P aller Permutationen von $\mathfrak{M}$. Man kann sich also auf den Standpunkt stellen, es handle sich bei den im Text formulierten Sätzen über Operatorgruppen um Permutationsgruppensätze, wie sie in jedem guten Algebralehrbuch zu finden sind. Aber die Einführung der Operatorgruppen scheint mir grundsätzlich zweckmäßig. Denn sie gestattet es vielfach (z. B. hier im Text), durchweg mit einer festen Gruppe G zu arbeiten; man braucht nicht immer wieder zu einer neuen, passenden Permutationsgruppen*darstellung* P_G von G überzugehen.

Die Elemente A, B aus $\mathfrak{M}$ heißen *relativ G konjugiert*, wenn $B = cA$ für ein $c \in G$. Andererseits nennen wir wie üblich die Untermengen U, V von G *in G konjugiert*, wenn $V = c \cdot U \cdot c^{-1}$ für ein $c \in G$. Es gilt dann:

$F_{uA} = u \cdot F_A \cdot u^{-1}$, d. h.: Die Fixgruppen zweier relativ G konjugierter Elemente aus $\mathfrak{M}$ sind in G konjugiert.

Unter der *Konjugiertenserie $\mathfrak{K}_A$ von A relativ G* verstehen wir die Menge aller zu A relativ G konjugierten Elemente $uA \in \mathfrak{M}$ $(u \in G)$. Offenbar ist $\mathfrak{K}_A = \mathfrak{K}_{uA}$, d. h. eine Konjugiertenserie ist durch jedes ihrer Elemente eindeutig bestimmt; also ist $\mathfrak{M}$ Vereinigung von paarweise elementfremden Konjugiertenserien. Ferner sieht man mühelos: Die Menge aller $u \in G$, die der Bedingung $uA = cA$ genügen, bildet die Linksnebenschar $c \cdot F_A$ von F_A. Die Elemente der Konjugiertenserie $\mathfrak{K}_A$ entsprechen also umkehrbar eindeutig den Linksnebenscharen $c \cdot F_A$ von F_A. Ist demnach speziell G endlich und bedeutet $i(G:F_A)$ den Index von F_A in G im üblichen Sinne, so gilt der Satz:

Die Elementezahl von K_A ist gleich $i(G:F_A)$.

Bei den folgenden Anwendungen ist $\mathfrak{M}$ stets eine *Menge von Untermengen* einer festen endlichen Gruppe G. Im übrigen aber sind zwei Fälle zu unterscheiden:

1. *Methode.* (Hier beschränken wir uns auf den Fall, daß $\mathfrak{M}$ aus *Untergruppen* von G besteht.) Das Kompositum aU $(a \in G,\ U \in \mathfrak{M})$ wird durch $aU = a \cdot U \cdot a^{-1}$ definiert. Hier ist F_U der *Normalisator $N(G:U)$ von U in G* im Sinne der üblichen Terminologie, $\mathfrak{K}_U$ eine Serie konjugierter Untergruppen in G, und wir haben wegen $F_U \supseteqq U$ den Satz:

Die Gliederzahl einer Konjugiertenserie $\mathfrak{K}_U$ in G ist stets ein Teiler von $i(G:U)$.

Gelegentlich beschränken wir uns auch darauf, daß wir nicht die volle Gruppe G, sondern nur eine Untergruppe H als Operatorgruppe (mit der Vorschrift $aU = a \cdot U \cdot a^{-1}$) auf die Menge $\mathfrak{M}$ wirken lassen. Dann nennen wir $\mathfrak{K}_U$ eine Serie von *relativ H in G* konjugierten Untergruppen. Hier wird offenbar $F_U = N(G:U) \cap H$ Untergruppe von H, und es gilt daher:

Die Gliederzahl einer Konjugiertenserie $\mathfrak{K}_U$ in G relativ H ist stets ein Teiler von $o(H)$.

2. *Methode*[3]. (Hier wird $\mathfrak{M}$ eine Menge von passenden *Untermengen*, nicht nur Untergruppen, von G sein.) Wir definieren aA $(a \in G,\ A \in \mathfrak{M})$ durch das *Komplexprodukt* im üblichen Sinne: $aA = a \cdot A$. Es gelten dann die Sätze:

1. *In jeder Konjugiertenserie $\mathfrak{K}_A$ gibt es mindestens ein A_0 mit $e \in A_0$* (trivial).

2. A ist stets Vereinigung einer gewissen Menge von Rechtsnebenscharen $F_A \cdot c$ von F_A; *es ist also $o(F_A)$ stets ein Teiler der Elementezahl $z(A)$ von A: $z(A) = t \cdot o(F_A)$, und die Gliederzahl von $\mathfrak{K}_A$ ist gleich $t \cdot o(G) \cdot z(A)^{-1}$.* (Man beachte: Aus $c \in A$ folgt $F_A \cdot c \subseteqq A$ wegen $F_A \cdot A = A$.)

[3]) Während die Anwendung der 1. Methode in der Gruppentheorie überall üblich ist, ist die Anwendung der 2. Methode zum Beweis des p-Gruppen-Existenzsatzes der entscheidende neue Gedanke von Herrn Wielandt.

3. *Ist* $o(F_A) = z(A)$, also $t = 1$ in den Formeln von 2., *und ist* $e \in c \cdot A = A_0$, *so ist* $F_{A_0} = A_0$, *und es besteht* $\mathfrak{K}_A = \mathfrak{K}_{A_0}$ *gerade aus der Gruppe* F_{A_0} *der Ordnung* $z(A)$ *und ihren Linksnebenscharen.* (Beachte: Wegen $o(F_{A_0}) = o(F_A) = z(A)$ ist A_0 gleich der einen, e enthaltenden Rechtsnebenschar von F_{A_0}. Die übrigen Elemente von $\mathfrak{K}_A$ haben die Gestalt $c \cdot A_0 = c \cdot F_{A_0}$.)

Es sei jetzt p eine Primzahl; $Z_{G,l}$ sei die Anzahl aller Untergruppen l-ter Ordnung von G. Dann beweisen wir zuerst:

Satz 1[4]. *Ist* $o(G) = p^r \cdot q$ *durch* p^r *teilbar, so gilt stets* $Z_{G,p^r} \equiv 1\,(p)$.

Zum Beweis sei $\mathfrak{M}$ die Menge aller Untermengen der Elementezahl p^r von G, es bedeute $Z_{\mathfrak{M}}$ die Elementezahl von $\mathfrak{M}$, und es werde G *nach der* 2. *Methode* zur Operatorgruppe auf $\mathfrak{M}$ gemacht. Aus den Bemerkungen 2 und 3 zur 2. Methode folgt dann sofort: Eine Konjugiertenserie $\mathfrak{K}_A$ aus $\mathfrak{M}$ relativ G hat entweder eine Gliederzahl $t \cdot q$, wobei t ein von 1 verschiedener Teiler von $z(A) = p^r$, also $t = p^s$ für ein s mit $1 \leqq s \leqq r$. Oder aber es hat $\mathfrak{K}_A$ genau die Gliederzahl q, und es besteht dann $\mathfrak{K}_A$ gerade aus einer Untergruppe p^r-ter Ordnung und ihren Linksnebenscharen. Da ferner jede Untergruppe p^r-ter Ordnung mit ihren Linksnebenscharen eine Serie aus $\mathfrak{K}_A$ bildet, erhalten wir:

$$Z_{\mathfrak{M}} \equiv Z_{G,p^r} \cdot q\,(p \cdot q)\,. \tag{1}$$

Andererseits ist

$$Z_{\mathfrak{M}} = \binom{p^r \cdot q}{p^r} = q \cdot \binom{p^r \cdot q - 1}{p^r - 1} \quad \text{und} \quad \binom{p^r \cdot q - 1}{p^r - 1} = \prod_{k=1}^{p^r - 1} p^r \cdot q \cdot k^{-1} - 1\,.$$

Da ferner k höchstens durch p^{r-1} teilbar ist, ergibt sich bei gekürzter Darstellung: $p^r \cdot q \cdot k^{-1} = p \cdot q_k \cdot l_k^{-1}$ mit $l_k \not\equiv 0\,(p)$. Die Ausmultiplikation der rechten Seite führt also zu einer Gleichung für $\binom{p^r \cdot q - 1}{p^r - 1}$ von der Form: $\binom{p^r \cdot q - 1}{p^r - 1} = (-1)^{p^r - 1} + p \cdot m\, l^{-1}$, wobei m und l teilerfremd und $l \not\equiv 0\,(p)$. Da aber $\binom{p^r \cdot q - 1}{p^r - 1}$ ganzzahlig ist, muß $l = 1$ sein; d. h. wir haben $\binom{p^r \cdot q - 1}{p^r - 1} \equiv (-1)^{p^r - 1} \equiv 1\,(p)$. Das bedeutet:

$$Z_{\mathfrak{M}} \equiv q\,(p \cdot q)\,. \tag{2}$$

Vergleich von (1) und (2) liefert: $Z_{G,p^r} \cdot q \equiv q\,(p \cdot q)$, $Z_{G,p^r} \equiv 1\,(p)$.

1. Korollar zu Satz 1. *Ist* p^r *ein Teiler von* $o(G)$, *so gibt es stets mindestens eine Untergruppe der Ordnung* p^r.

2. Korollar zu Satz 1. *Ist* p^r *ein Teiler von* $o(G)$, *so gibt es mindestens eine Serie* $\{U_1, \ldots, U_s\}$ *in* G *konjugierter Untergruppen* (im Sinne der 1. Methode), *bei der* $s \not\equiv 0\,(p)$.

---

[4]) Vgl. Frobenius, S.-Ber. Preuß. Akad. Wiss. Berlin 981—993 (1895).

Satz 2.[5]) *Es sei* $o(G) = p^s$, *also* G *eine* p*-Gruppe*; $Z^{(i)}_{G,p^r}$ *sei die Anzahl der invarianten Untergruppen* p^r*-ter Ordnung von* G $(r \leqq s)$. *Dann ist* $Z^{(i)}_{G,p^r} \equiv 1\,(p)$.

Zum Beweis machen wir G nach der 1. Methode zur Operatorgruppe auf der Menge $\mathfrak{N}$ aller Untergruppen p^r-ten Grades von G, wir teilen also $\mathfrak{N}$ in Serien $\mathfrak{K}_U$ *in* G konjugierter Gruppen ein. Aus den Bemerkungen zur 1. Methode folgt sofort: Ist nicht die Gliederzahl von $\mathfrak{K}_U$ gleich 1 — ein Fall, der dann und nur dann eintritt, wenn U in G invariant ist —, so ist die Gliederzahl von $\mathfrak{K}_U$ eine positive p-Potenz. Das heißt, wir haben für die Elementezahl Z_{G,p^r} von $\mathfrak{N}$ die Kongruenz $Z_{G,p^r} \equiv Z^{(i)}_{G,p^r}$ (p); aus Satz 1 folgt also Satz 2.

Satz 3. *Ist* $o(G) = p^{s^*}$, $U \subseteqq G$ *und* $o(U) = p^r$ *für ein* $r < s^*$, *so gibt es stets ein* V *mit* $G \supseteqq V \supset U$, $o(V) = p^{r+1}$.

Für $s^* = 1$ ist die Behauptung trivial, wir dürfen also ihre Richtigkeit für alle Gruppen $\tilde{G}$ mit $o(\tilde{G}) = p^{s^*-1}$ voraussetzen. Enthält nun U eine invariante Untergruppe I von G der Ordnung p, so folgt Satz 3 für U durch Induktion nach Übergang zu $\tilde{G} = G/I$, $\tilde{U} = U/I$. Enthält aber U kein in G invariantes I mit $o(I) = p$, so sei I irgendeine (nach Satz 2 existierende) invariante Untergruppe p-ter Ordnung von G. Wegen der Invarianz von I in G wird das Komplexprodukt $I \cdot U$ eine Gruppe, und wir haben

$$o(I \cdot U) = o(I) \cdot o(U) \cdot o(I \cap U)^{-1} = p^{1+r} \text{ wegen } o(I \cap U) = o(\{e\}) = 1\,.$$

Satz 4. *Ist* $G \supseteqq I_1 \supset I_2$, *wobei* I_1 *und* I_2 *in* G *invariant sind, und hat man*

$$o(G) = p^{s^*}, \quad o(I_k) = p^{r_k} \quad (k = 1, 2;\, r_1 - 2 \geqq r_2 \geqq 0)\,,$$

so gibt es stets eine in G *invariante Untergruppe* I *mit* $I_1 \supset I \supset I_2$, $o(I) = p^{r_1-1}$.

Beim Beweis dürfen wir $I_2 = \{e\}$ annehmen, da andernfalls Übergang zu G/I_2, I_1/I_2 möglich wäre. Wir dürfen also die Bedingung $I \supseteqq I_2$ vernachlässigen. Es sei $\mathfrak{M} = \{U_1, \ldots, U_s\}$ die Menge aller Untergruppen p^{r_1-1}-ter Ordnung von I_1. Dann gehört wegen der Invarianz von I_1 in G für jedes U_i die ganze Serie $\mathfrak{K}_{U_i}$ der zu U_i in G konjugierten Gruppen zu $\mathfrak{M}$. Da ferner $s \equiv 1\,(p)$, folgt genau so wie bei Satz 2 die Existenz eines in G invarianten U_i.

Nennen wir eine Kette $G = I_0 \supset I_1 \supset \ldots \supset I_t = \{e\}$ eine *Hauptreihe* von G, wenn alle I_k *in* G invariant sind und wenn sich für kein $k \leqq t$ zwischen I_{k-1} und I_k eine echte, in G invariante Zwischengruppe einschieben läßt, so folgt aus Satz 4 sofort:

Korollar zu Satz 4. *Ist* $o(G) = p^{s^*}$, *so ist bei jeder Hauptreihe* $G = I_0 \supset I_1 \supset \ldots \supset I_s = \{e\}$ *stets* $s = s^*$, $o(I_{k-1}/I_k) = p$ $(k = 1, \ldots, s)$.

G ist also in der üblichen Terminologie nicht nur auflösbar, sondern sogar *überauflösbar*. (Man beachte, daß zur Herleitung des Korollars weder der Begriff des Zentrums eingeführt noch auf die allgemeine Theorie der Hauptreihen zurückgegriffen werden mußte.)

---

[5]) Vgl. Burnside, Theory of Groups of finite order, 2nd ed. Cambridge 1911, p. 129.

Wir wenden uns jetzt wieder der Untersuchung von Gruppen G beliebiger Ordnung zu. Das folgende Theorem hat mehr den Charakter eines Hilfssatzes[6]):

Satz 5. *Es sei* $\{U_1, \dots, U_s\}$ *irgendeine Serie in* G *konjugierter Untergruppen mit* $s \not\equiv 0(p)$; V *sei eine weitere Untergruppe mit* $o(V) = p^t$. *Dann gibt es mindestens ein* U_i *derart, daß* $N(G : U_i) \supseteqq V$, *daß also* $v \cdot U_i \cdot v^{-1} = U_i$ *für alle* $v \in V$ *wird.*

Nach der verallgemeinerten 1. Methode teilen wir $\{U_1, \dots, U_s\}$ in Serien *relativ* V *in* G konjugierter Gruppen ein. Aus den Bemerkungen zur 1. Methode folgt analog wie bei Satz 2: Entweder es besteht $\mathfrak{K}_{U_i}$ nur aus einem Element, oder es ist die Gliederzahl von $\mathfrak{K}_{U_i}$ eine positive p-Potenz. Wegen $s \not\equiv 0(p)$ muß für mindestens ein U_i der erste Fall eintreten. Dann aber wird $v \cdot U_i \cdot v^{-1} = U_i$ für alle $v \in V$ nach Definition.

Wie üblich nennen wir die Untergruppe S der Ordnung p^{s^*} eine *p-Sylowgruppe* von G, wenn p^{s^*} die höchste in $o(G) = p^{s^*}q$ aufgehende p-Potenz, also $q \not\equiv 0(p)$ ist.

Satz 6. *Jede p-Untergruppe von* G *ist Untergruppe einer p-Sylowgruppe von* G. *Alle p-Sylowgruppen von* G *sind in* G *konjugiert.*

Beweis. Nach dem 2. Korollar zu Satz 1 gibt es eine Serie $\{S_1, \dots, S_s\}$ in G konjugierter Sylowgruppen mit $s \not\equiv 0(p)$. Ist V eine p-Untergruppe von G, wobei etwa $o(V) = p^r$, so existiert nach Satz 5 ein S_i derart, daß $v \cdot S_i \cdot v^{-1} = S_i$ für alle $v \in V$. Daraus folgt (ähnlich wie bei Satz 2): $V \cdot S_i$ ist eine Gruppe, und man hat

$$o(V \cdot S_i) = o(V) \cdot o(S_i) \cdot o(V \cap S_i)^{-1} = p^{r+s^*} \cdot o(V \cap S_i)^{-1}.$$

Wegen $o(G) \not\equiv 0\ (p^{1+s^*})$ ergibt sich weiter:

$$o(V \cap S_i) = p^r = o(V), \quad V = V \cap S_i, \quad V \subseteqq S_i.$$

Ist schließlich speziell $V = S$ eine p-Sylowgruppe von G, so haben wir:

$$r = s^*, \quad o(V \cap S_i) = o(S_i); \quad S_i = V \cap S_i = V.$$

Kombiniert man Satz 6 und Satz 3, so erhält man:

Korollar zu Satz 6. *Ist* $U \subseteqq G$, $o(U) = p^r$ *und* $r < s^*$, *so gibt es stets ein* V *mit* $G \supseteqq V \supset U$ *und* $o(V) = p^{r+1}$.

Satz 7. *Es sei* $G = I_n \supset I_{n-1} \supset \dots \supset I_1$, *wobei* I_{k-1} *invariant in* I_k *und*

$$o(I_k/I_{k-1}) \not\equiv 0\ (p) \quad (k = 1, \dots, n).$$

Dann sind (für $o(I_1) \equiv 0\ (p)$*) die sämtlichen p-Sylowgruppen* $S_1, \dots, S_s$ *von* I_1 *gleichzeitig auch die sämtlichen p-Sylowgruppen von* G.

Es genügt offenbar, die Behauptung für $n = 2$ zu beweisen. Wegen $o(I_2/I_1) \not\equiv 0$ (p) sind $S_1, \dots, S_s$ nicht nur in I_1 sondern auch in I_2 Sylowgruppen. Aus $u \cdot I_1 \cdot u^{-1} =$

[6]) Die Herleitung der Sätze 1 bis 4 samt ihren Korollaren war das Hauptziel der Note. Im folgenden soll nur gezeigt werden, daß der anschließende Beweis der noch ausstehenden Sylowgruppensätze noch etwas einfacher und durchsichtiger gestaltet werden kann als es z. B. in dem Lehrbuch von Zassenhaus schon der Fall war.

$= I_1$ ($u \in I_2$) folgt ferner, daß für $i = 1, \ldots, s$ stets $u \cdot S_i \cdot u^{-1}$ ebenso wie S_i eine p-Sylowgruppe von I_1 und damit ein Element von $\{S_1, \ldots, S_s\}$ sein muß. Das heißt also, die S_i bilden nicht nur in I_1 sondern auch in I_2 eine volle Serie konjugierter Untergruppen; nach Satz 6 gibt es also außer ihnen in I_2 keine weitere p-Sylowgruppe.

1. Korollar zu Satz 7. *Ist* $G = I_n \supset I_{n-1} \supset \ldots \supset I_1$, *wobei* I_{k-1} *in* I_k *invariant,* $o(I_k/I_{k-1}) \not\equiv 0\ (p)$, $o(I_1) = p^{s^*}$ $(k = 1, \ldots, n)$, *so ist* I_1 *die einzige p-Sylowgruppe von G und damit in G invariant.*

2. Korollar zu Satz 7. *Ist S eine p-Sylowgruppe von G und* $T = N(G:S)$, $T_1 = N(G:T)$, *so ist* $T = T_1$.

(Man beachte die Definition des Normalisators $N(G:U)$ und die Tatsache, daß S nach dem 1. Korollar in T_1 invariant ist.)

Eingegangen am 15. 7. 1960

Anschrift des Autors:
Wolfgang Krull
Bonn, Meckenheimer Allee 81

On a Finite Matrix Representation of the Braid Group

By

Seymour Lipschutz *)

1. Introduction. There exists a finite matrix representation of the Braid Group B_n (see Section 2). Here we consider B_n to be a group of automorphisms of a free group F [1]. It can be shown, due to results of Magnus [6], that the faithfulness of the above matrix representation depends upon the faithfulness of the matrix representation of a subgroup R of B_n — a subgroup with important topological properties [6]. Further, it has been shown by Gassner [3] that the kernel of the above representation is contained in the subgroup of braids which induce the identical automorphism in F/F'', where F'' is the second derived group of F.

In this paper we prove, by a suitable change in the basis of F, that the matrix representation of R is pairwise free. We also show as a result of a recursion formula (after analyzing the effect of R on the nontrivial terms of an expansion of F in a Lie ring) that there are elements in each of the members of the derived series of R which are not contained in the kernel of the matrix representation of B_n.

2. The matrix representation. Let A be a group of automorphisms of a free group F with free generators $x_1, \ldots, x_n$. If, for every α in A,

$$\alpha(x_i) = W_i(x_\lambda), \quad \sum(\text{exponents of } x_j \text{ in } W_i) = \delta_{ij}, \tag{2.1}$$

we show it is possible to associate a matrix with α.

First we associate

$$x_i \leftrightarrow \begin{pmatrix} t_i & s_i \\ 0 & 1 \end{pmatrix}, \quad x_i^{-1} \leftrightarrow \begin{pmatrix} t_i^{-1} & -t_i^{-1} s_i \\ 0 & 1 \end{pmatrix}$$

where the t_i, s_i are indeterminants. The above association can be shown to be a faithful representation of F/F'' (see [5]). Then, in view of (2.1), α induces the following

$$\alpha\begin{pmatrix} t_i & s_i \\ 0 & 1 \end{pmatrix} = W_i\left(\begin{pmatrix} t_\lambda & s_\lambda \\ 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} t_i & A_{i1} s_1 + \cdots + A_{in} s_n \\ 0 & 1 \end{pmatrix} \tag{2.2}$$

which induces

$$\alpha(s_i) = \sum_{j=1}^{n} A_{ij} s_j \qquad (i = 1, 2, \ldots, n),$$

* Work on this paper was sponsored in part by a grant from the National Science Foundation, NSF-G 9659.

where the A_{ij} are polynomials in $t_i^{\pm 1}$. (The reader can easily check that the product in (2.2) does have the form on the right.) It is the matrix (A_{ij}) that we finally associate with α.

Note. If we consider the free module generated by the $\{s_i\}$ with the polynomials in $t_i^{\pm 1}$ as a ring of operators then α introduces an automorphism which leaves the ring of operators element-wise fixed. From this it follows that these automorphisms represented by the matrices (A_{ij}) does, indeed, give a representation of A.

Now, if α is a braid in the subgroup A_n of B_n for which

$$B_n / A_n \cong \Sigma_n = \text{symmetric group of order } n!,$$

then it is well known that, as an automorphism of F,

$$\alpha(x_i) = T_i(x_\lambda)\, x_i\, T_i(x_\lambda)^{-1}, \tag{2.3}$$
$$\alpha(x_1 \cdots x_n) = x_1 \cdots x_n,$$

which is of the form (2.1). Thus we have a finite matrix representation for A_n.

Since B_n/A_n is of finite order there exists a standard method [8] to extend the matrix representation of A_n to a finite matrix representation of B_n.

3. The subgroup *R*. Let R be the subgroup of B_n generated by the braids

$$R_i = (\sigma_1 \sigma_2 \cdots \sigma_{i-2})^{i-1} (\sigma_i \cdots \sigma_{n-1})^{i-n} \qquad (i = 2, 3, \ldots, n+1), \tag{3.1}$$

where the $\{\sigma_i\}$ are the usual generators of B_n. (The braid σ_i is the following automorphism of F, the free group on which B_n acts.

$$\sigma_i(x_j) = x_j, \text{ if } j \neq i, i+1, \tag{3.2}$$
$$\sigma_i(x_i) = x_{i+1},$$
$$\sigma_i(x_{i+1}) = x_{i+1}{}^{-1} x_i x_{i+1}\,.)$$

Figure 1. R_5 in B_7.

Figure 1 shows the projection of a typical braid of R. It is well known that $R_{n+1} = C$ generates the center of B_n and that the other $\{R_i\}$ are free. (The reader will note that there is a subgroup R defined for each n. We will use the same letter R to denote any or all of them.)

In order to simplify our formulas we introduce the notation:

$$\bar{x} = x^{-1},$$
$$b_i = x_i x_{i+1} \cdots x_n,$$
$$a_{ij} = \begin{cases} b_1 & \text{if } j < i, \\ I, \text{ the identity} & \text{if } i \leqq j. \end{cases}$$

It can now be shown, using (3.1) and (3.2), that

$$R_i(x_j) = b_i \bar{a}_{ij} x_j a_{ij} \bar{b}_i, \tag{3.3}$$
$$R_i(b_j) = b_i \bar{a}_{ij} b_j \bar{b}_i a_{ij},$$

which are of the form (2.1). Thus we have a matrix representation of R using the $\{b_i\}$ as generators of F.

Theorem 1. *The matrices corresponding to the above generators of R are pair-wise free.*

Proof. Let R_i, R_j be two such generators. Say $i < j$. After permuting the i^{th} and $(j-1)^{\text{th}}$ rows and columns in the matrices, we see that the following submatrices multiply independent from the rest of the matrix:

$$\begin{pmatrix} 1 & 0 \\ 1 - t_j & t_i \end{pmatrix} \in R_i, \quad \begin{pmatrix} \bar{t}_1 t_j & 1 - \bar{t}_1 t_{j-1} \\ 0 & 1 \end{pmatrix} \in R_j. \tag{3.4}$$

Let $t_i = 1, t_1 = t_{j-1} = t_j = -1$ in (3.4). Then we have

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},$$

which are known to be free. (See [7].)

4. The Lie ring presentation. We use the commutator notation:

$$[f, g] = \bar{f}\bar{g} f g \quad (\text{or } fg - gf),$$
$$[f_1, f_2, \ldots, f_n] = [\cdots[[f_1, f_2], f_3], \ldots, f_n],$$
$$[f, g^k] = [f, g^{k-1}, g],$$

where we call n the *weight* of the commutator (or the *degree* if it is a term in a Lie ring).

There is a known presentation of F in terms of a free ring P with generators $\{u_i\}$ by associating $x_i \leftrightarrow e^{u_i}$. We can then study the action of R on F in terms of automorphisms of P. If

$$\beta(x_i) = x_{j_1} \cdots x_{j_n} x_i \bar{x}_{j_n} \cdots \bar{x}_{j_1},$$

β in R, then

$$\beta(u_i) = \sum_{k_{j_1}, \ldots, k_{j_n} = 0}^{\infty} \frac{\left[u_i, u_{j_1}^{k_{j_1}}, \ldots, u_{j_n}^{k_{j_n}}\right]}{k_{j_1}! \ldots k_{j_n}!}. \tag{4.1}$$

The above formula is based upon the fact that, in a free ring with generators u, v, $e^u e^v e^{-u} = e^w$, where $w = v +$ Lie elements in the ring. (For a more complete discussion of this presentation of F see [4].)

Since we are mainly interested in the action of R on F/F'', we set all commutators of commutators in P equal to zero. Therefore, using the Jacobi identity, we are now allowed to commute generators after the second in any term of a Lie element. Also, as a result, the reader can easily verify this important identity:

$$\beta([u_1, u_2, \ldots, u_n]) = [\beta(u_1), u_2, \ldots, u_n] - [\beta(u_2), u_1, u_3, \ldots, u_n] - [u_1, u_2, \ldots, u_n]. \tag{4.2}$$

We now only consider the braid group B_4 and its subgroup R (generated by R_2, R_3, R_4 and R_5). We see that $[R_4, R_3]$, $[R_3, R_2]$, $[R_4, R_2]$, which we denote by S_1, S_2, S_3 respectively, are in the first derived group of R. If we let $T_1 = [S_1, S_2]$, $T_2 = [S_1, S_3]$, $T_3 = [S_2, S_3]$ then we also notice that $[T_2, T_1]$, $[T_3, T_1]$, $[T_3, T_2]$ are in the third derived group of R.

Using (3.3), (4.1) and (4.2), we compute the automorphisms of the free ring P by the above elements of R. Tables 1, 2 and 3, where the notation $a = u_1, b = u_2, c = u_3, d = u_4$ and

$$a_1 a_2 \cdots a_n = [a_1, a_2, \ldots, a_n],$$
$$A = abcd(a + b + c + d)^2$$

is used, indicate the elements of P onto which the generators on the left are mapped by the automorphisms in the top row.

Table 1

	R_2	R_3	R_4
$a \to$	a	$a + ba + \cdots$	$a + ba + ca + \cdots$
$b \to$	$b + bd + bc + \cdots$	$b + ab + \cdots$	$b + ab + cb + \cdots$
$c \to$	$c + cd + cb + \cdots$	$c + cd + \cdots$	$c + ac + bc + \cdots$
$d \to$	$d + dc + db + \cdots$	$d + dc + \cdots$	d

Table 2

	$S_1 = [R_4, R_3]$	$S_2 = [R_3, R_2]$	$S_3 = [R_4, R_2]$
$a \to$	$a + dca + \cdots$	$a + cba + dba + \cdots$	$a + dba + dca + \cdots$
$b \to$	$b + dcb + \cdots$	$b + acb + adb + \cdots$	$b + adb + \cdots$
$c \to$	$c + adc + bdc + \cdots$	$c + bac + \cdots$	$c + adc + \cdots$
$d \to$	$d + cad + cbd + \cdots$	$d + bad + \cdots$	$d + cad + bad + \cdots$

Table 3

	$[T_2, T_1]$	$[T_3, T_1]$	$[T_3, T_2]$
$a \to$	$a + dcaA + \cdots$	$a + cbaA + dbaA + \cdots$	$a + dbaA + dcaA + \cdots$
$b \to$	$b + dcbA + \cdots$	$b + acbA + adbA + \cdots$	$b + adbA + \cdots$
$c \to$	$c + adcA + bdcA + \cdots$	$c + bacA + \cdots$	$c + adcA + \cdots$
$d \to$	$d + cadA + cbdA + \cdots$	$d + badA + \cdots$	$d + cadA + badA + \cdots$

Theorem 2[1]. *There are elements in every member of the derived series of the subgroup R of the braid group B_4 which do not induce the identical automorphism in F/F''.*

Proof. Follows directly from the recursion formulas in Table 2 and Table 3.

[1] The author has also proven this result for the lower central series of R.

5. Magnus' results. We prove, using results by Magnus [6], the following

Lemma. *If the matrix representations of A_{n-1} in B_{n-1} and of R in B_n are faithful then the matrix representation of A_n is also faithful.*

Proof. Let K_n be the kernel of the matrix representation of A_n, the subgroup of B_n for which $B_n/A_n \simeq \Sigma_n =$ the symmetric group of order $n!$. (See Section 2.) We want to show that

$$K_n \cap R = 1, A_{n-1} \cap K_n = 1 \Rightarrow K_n = 1. \tag{5.1}$$

Let Z_n be the normal divisor of F_n generated by $x_1 x_2 \cdots x_n$. (F_n, freely generated by $x_1, \ldots, x_n$, is the free group on which B_n acts.) Since Z_n is characteristic under A_n, we know that A_n acts on F_n/Z_n. We call A_n^* the group of automorphisms of F_n/Z_n induced by A_n. Magnus showed that

$$\begin{aligned} A_n^* &\cong A_n/C_n, \\ A_n^* &\cong A_{n-1} \cdot I_{n-1}, \\ A_{n-1} \cap I_{n-1} &= C_{n-1}, \end{aligned} \tag{5.2}$$

where I_{n-1}, generated freely by $R_2, \ldots, R_n$, is the group of inner automorphisms of $F_{n-1} = F_n/Z_n$ and a normal divisor of A_n^*, and where C_n is the center of B_n. (Note. C_n is known to be generated by $R_{n+1} = (\sigma_1 \cdots \sigma_{n-1})^n$ so $R = I_{n-1} \times C_n$.)

By (5.2),

$$A_n = A_{n-1} \cdot (I_{n-1} \times C_n) \equiv A_{n-1} \cdot R.$$

Therefore

$$A_n/K_n = (A_{n-1} \cdot R)/K_n \,|\, A_{n-1}/(K_n \cap A_{n-1})| \;\; |R/K_n \cap R)|. \tag{5.3}$$

By (5.2) and (5.3) it follows that (5.1) is true.

Theorem 3. *The faithfulness of the matrix representations for all R imply the faithfulness for all B_n.*

Proof. By the way we extend our matrix representation of A_n to a matrix representation of B_n, it is only necessary to show that the theorem is true for all A_n.

The proof, by induction, follows directly from the lemma and the fact that the matrix representation of A_3 is known to be faithful.

6. Summary of results. We have proven the following:

(1) *The faithfulness of the matrix representation of B_n depends upon the faithfulness of the representation for R.*

(2) *The matrix representation is pair-wise faithful for the generators of R.*

(3) *There are braids in every member of the derived series of R in B_4 which are not contained in the kernel of the matrix representation.*

Our conjecture, that the finite matrix representation of B_n is faithful, seems reasonable. If this is true, then this could be one method towards solving the transformation problem for the Braid group.

Bibliography

[1] E. Artin, Theory of Braids. Ann. of Math. **48**, 101–126 (1947).
[2] E. Artin, Theorie der Zöpfe. Abh. Math. Sem. Univ. Hamburg **4**, 47–72 (1925).
[3] B. J. Gassner, On Braids. To be published in Abh. Math. Sem. Univ. Hamburg (1961).
[4] W. Magnus, On the Exponential Solution of Differential Equations for a Linear Operator. Comm. Pure Appl. Math. **7**, 649–673 (1954).
[5] W. Magnus, On a Theorem of Marshall Hall. Ann. of Math. **40**, 764–768 (1939).
[6] W. Magnus, Über Automorphismen von Fundamentalgruppen berandeter Flächen. Math. Ann. **109**, 617–646 (1934).
[7] W. Magnus, Untersuchungen über einige unendliche diskontinuierliche Gruppen. Math. Ann. **105**, 52–74 (1931).
[8] A. Speiser, Theorie der Gruppen von endlicher Ordnung. 3rd Edition, Berlin 1936.

Eingegangen am 3. 5. 1960

Anschrift des Autors:

Seymour Lipschutz
25 Waverly Place
Department of Mathematics
New York University
New York (N.Y.), USA

Charakteristisches Polynom, Determinante und Spur als Abbildungsfunktionen

Von

PETER WILKER

1. Sei A eine lineare Abbildung eines endlich-dimensionalen Vektorraums $\mathfrak{R}$ über einem Körper K in sich. Man kann die Methoden, die Determinante $|A|$ von A zu erklären, in zwei Klassen einteilen. Die indirekten Methoden ordnen zuerst nach Wahl einer Basis von $\mathfrak{R}$ der Abbildung A eine Matrix mit Elementen aus K zu. Die Determinante dieser Matrix kann dann auf eine der zahlreichen bekannten Arten definiert werden (Methoden von LEIBNIZ-CRAMER, GRASSMANN-WEIERSTRASS; vgl. für andere Wege, auch im nicht-kommutativen Fall, [4], § 13, für eine vom Verfasser vorgeschlagene rekursive Definition [5]). Anschließend ist zu zeigen, daß der erhaltene Wert $|A|$ von der Wahl der Basis von $\mathfrak{R}$ unabhängig ist. Die Methode von GRASSMANN-WEIERSTRASS läßt sich zu einer direkten ausgestalten, indem man die äußere Potenz $\overset{n}{\wedge} A$ $(n = \dim \mathfrak{R})$ bildet, die eine lineare Abbildung der 1-dimensionalen äußeren Potenz $\overset{n}{\wedge} \mathfrak{R}$ in sich ist, also die Form $x \to \delta x (x \in \overset{n}{\wedge} \mathfrak{R}, \delta \in K)$ hat; man erklärt $|A| = \delta$ (vgl. etwa [4], §§ 12, 13 oder [2b], § 53; eine andere direkte Methode in [1]). Ganz analog wird auch die Spur von A entweder indirekt über die Diagonalelemente der zugeordneten Matrizen oder direkt durch Heranziehung von Tensorprodukten erklärt (vgl. [4], § 11 oder [2b], § 56, Ex. 4).

Die eben erwähnte, direkte Methode hat den Vorteil, daß sie sich auf Moduln über Ringen in gleicher Weise durchführen läßt wie auf Vektorräumen. Von der üblichen Theorie der linearen Abbildungen von Vektorräumen aus gesehen kann sie allerdings als ein Umweg betrachtet werden und es mag wünschenswert sein, eine direkte Definition zu gewinnen, die sich, unter Verwendung spezifischer Hilfsmittel dieser Theorie, ganz in deren Rahmen hält und Anleihen bei der multilinearen Algebra vermeidet. Die nachstehend durchgeführte Methode geht, umgekehrt wie die oben erwähnten, vom charakteristischen Polynom aus, das als Funktion über der Menge der Abbildungen endlich-dimensionaler Vektorräume erklärt wird, und führt an dieses anschließend Determinante und Spur als ebensolche Funktionen ein. Die wichtigsten elementaren Eigenschaften der drei Funktionen werden dann auf demselben direkten Weg bewiesen.

Die nachfolgenden Ausführungen stützen sich auf einige einfache Ergebnisse der Zerlegungstheorie linearer Abbildungen, die kurz zusammengestellt werden mögen. Die Beweise finden sich z. B. in [3]; die nachstehend in eckiger Klammer beigefügten Zahlen verweisen auf die einschlägigen Abschnitte dieses Werks.

Es bezeichne im folgenden $(A, \mathfrak{R})$ eine lineare Abbildung eines endlich-dimensionalen Vektorraumes $\mathfrak{R}$ in sich; $\mathfrak{R}$ sei dabei über einem kommutativen Körper K erklärt, der, falls nichts anderes bemerkt, stets fest bleibt. Unter „Abbildungsfunktion" wird eine eindeutige Funktion $\varphi(A, \mathfrak{R})$ bzw. $\varphi(A, \mathfrak{R}, x)$ verstanden, erklärt über der Menge aller $(A, \mathfrak{R})$ mit Werten in K bzw. im Polynombereich $K[x]$. Der höchste Koeffizient von $\varphi(A, \mathfrak{R}, x)$ werde stets zu 1 angenommen.

Das „Ordnungspolynom" eines Vektors $r \in \mathfrak{R}$ bzgl. A ist dasjenige Polynom $\omega(x)$ kleinsten Grades (mit höchstem Koeffizienten 1), für welches $\omega(A)r = 0$ gilt [III 2]. Das „Minimalpolynom" $\mu(A, \mathfrak{R}, x)$ der Abbildung $(A, \mathfrak{R})$ ist das Polynom kleinsten Grades mit $\mu(A, \mathfrak{R}, A) = 0$; es ist ein Vielfaches jedes Ordnungspolynoms bzgl. $(A, \mathfrak{R})$, teilt hingegen alle Polynome $\varphi(x)$, für welche $\varphi(A) = 0$ gilt [III 1].

Eine Abbildung $(A, \mathfrak{R})$ heißt „zyklisch", falls ein Vektor $a \in \mathfrak{R}$ so existiert, daß $\mathfrak{R}$ durch die Vektoren a, Aa, $A^2a, \ldots$ erzeugt wird; a heißt dementsprechend „erzeugender Vektor" [III 2]. $(A, \mathfrak{R})$ ist dann und nur dann zyklisch, wenn der Grad von $\mu(A, \mathfrak{R}, x)$ gleich ist der Dimension von $\mathfrak{R}$ [III 4].

Eine „Zerlegung" der Abbildung $(A, \mathfrak{R})$ in der Form $(A, \mathfrak{R}) = \sum\limits_1^k (A_i, \mathfrak{R}_i)$ bedeute, daß sich $\mathfrak{R}$ als direkte Summe $\mathfrak{R} = \sum\limits_1^k \mathfrak{R}_i$ von bei A invarianten Unterräumen $\mathfrak{R}_i$ darstellen läßt und daß A_i die von A auf $\mathfrak{R}_i$ induzierte Abbildung ist. Sei $\mu(A, \mathfrak{R}, x) = \pi_1(x)^{r_1} \ldots \pi_m(x)^{r_m}$ die Primfaktorenzerlegung von μ, $\pi_i(x)$ irreduzibel über $K[x]$. Es gibt dann die „primäre Zerlegung" $(A, \mathfrak{R}) = \sum\limits_1^m (A_i, \mathfrak{R}_i)$, wobei $\mu(A_i, \mathfrak{R}_i, x) = \pi_i(x)^{r_i}$ ist und $\mathfrak{R}_i$ alle diejenigen Vektoren von $\mathfrak{R}$ enthält, deren Ordnungspolynom eine Potenz von $\pi_i(x)$ ist [IV 8].

Jede Abbildung $(A, \mathfrak{R})$ ist „vollständig zerlegbar", d. h. sie läßt eine Darstellung $(A, \mathfrak{R}) = \sum\limits_1^k (A_i, R_i)$ mit unzerlegbaren $(A_i, \mathfrak{R}_i)$ zu. Das Minimalpolynom einer unzerlegbaren Abbildung ist Potenz eines über $K[x]$ irreduziblen Polynoms [IV 8]. Die für das Folgende entscheidende Tatsache besagt weiter, daß eine unzerlegbare Abbildung $(A, \mathfrak{R})$ zyklisch und daher der Grad ihres Minimalpolynoms $\mu(A, R, x) = \pi(x)^r$, $\pi(x)$ irreduzibel in $K[x]$, gleich dim $\mathfrak{R}$ ist. Diese Tatsache folgt aus der allgemeinen Zerlegungstheorie [IV 7], läßt sich aber unschwer auch direkt, etwa durch vollständige Induktion nach dem Exponenten r, beweisen.

2. Die anschließend durchgeführte Definition des charakteristischen Polynoms stützt sich auf den folgenden

Satz 1. *Sei* $(A, \mathfrak{R}) = \sum\limits_1^k (A_i, \mathfrak{R}_i)$ *eine vollständige Zerlegung einer gegebenen linearen Abbildung* $(A, \mathfrak{R})$. *Aus den Minimalpolynomen* $\mu(A_i, \mathfrak{R}_i, x)$ *werde das Produkt*

$$\prod_1^k \mu(A_i, \mathfrak{R}_i, x)$$

gebildet. Führt man dies für alle vollständigen Zerlegungen von $(A, \mathfrak{R})$ *durch, so erhält man stets dasselbe Polynom* $\chi(A, \mathfrak{R}, x)$ *vom Grad* dim $\mathfrak{R}$.

Beweis. Betrachtet man zuerst die primäre Zerlegung von $(A, \mathfrak{R})$, so erkennt man sofort, daß es genügt, Satz 1 für Abbildungen $(A, \mathfrak{R})$ mit $\mu(A, \mathfrak{R}, x) = \pi(x)^r$, $\pi(x)$ irreduzibel in $K[x]$, abzuleiten. Bei jeder vollständigen Zerlegung $(A, \mathfrak{R}) = \sum\limits_1^m (A_i, \mathfrak{R}_i)$ einer solchen Abbildung treten als Minimalpolynome ebenfalls nur Potenzen desselben $\pi(x)$ auf, etwa $\mu(A_i, \mathfrak{R}_i, x) = \pi(x)^{r_i}$, und man hat stets $\prod\limits_1^m \mu(A_i, \mathfrak{R}_i, x) = \pi(x)^s$ mit $s = \sum\limits_1^m r_i$. Hat $\pi(x)$ den Grad p, so gilt nach dem am Schluß von 1. erwähnten Sachverhalt $\dim \mathfrak{R}_i = p r_i$, also $\sum\limits_1^m p r_i = ps = \dim \mathfrak{R}$. Damit erweist sich die Zahl s und daher auch $\chi(A, \mathfrak{R}, x) = \pi(x)^s$ als von der gewählten vollständigen Zerlegung unabhängig.

3. Eine Abbildungsfunktion $\varphi(A, \mathfrak{R}, x)$ heiße „multiplikativ", wenn jede Zerlegung $(A, \mathfrak{R}) = (A_1, \mathfrak{R}_1) + (A_2, \mathfrak{R}_2)$ die Gleichung $\varphi(A, \mathfrak{R}, x) = \varphi(A_1, \mathfrak{R}_1, x) \cdot \varphi(A_2, \mathfrak{R}_2, x)$ nach sich zieht. Weiter werde wie üblich als „Annihilator von $(A, \mathfrak{R})$" das Ideal der Polynome $\alpha(x) \in K[x]$ mit $\alpha(A) = 0$ bezeichnet; wie erwähnt ist jedes solche $\alpha(x)$ ein Vielfaches von $\mu(A, \mathfrak{R}, x)$.

Es mögen nun Abbildungsfunktionen $\varkappa(A, \mathfrak{R}, x)$ betrachtet werden, die den folgenden beiden Forderungen genügen:

I. $\varkappa$ ist multiplikativ;

II. $\varkappa$ gehört zum Annihilator von $(A, \mathfrak{R})$.

Nach II ist $\varkappa$ ein Vielfaches von μ, etwa $\varkappa(A, \mathfrak{R}, x) = \varkappa'(A, \mathfrak{R}, x)\, \mu(A, \mathfrak{R}, x)$ und aus I folgert man leicht, daß der Grad von $\varkappa$ mindestens gleich $\dim \mathfrak{R}$ sein muß. Es gilt genauer:

Satz 2. *Die in Satz* 1 *betrachtete Abbildungsfunktion* $\chi(A, \mathfrak{R}, x)$ *genügt* I *und* II; *jedes* $\varkappa(A, \mathfrak{R}, x)$, *das* I *und* II *erfüllt, ist ein Vielfaches von* $\chi(A, \mathfrak{R}, x)$.

Beweis. Die Richtigkeit der ersten Behauptung ist leicht einzusehen. Ist $(A, \mathfrak{R}) = \sum\limits_1^m (A_i, \mathfrak{R}_i)$ eine vollständige Zerlegung von $(A, \mathfrak{R})$, so ist

$$\varkappa(A, \mathfrak{R}, x) = \prod_1^m \varkappa'(A_i, \mathfrak{R}_i, x)\, \mu(A_i, \mathfrak{R}_i, x) = \Big(\prod_1^m \varkappa_i(A_i, \mathfrak{R}_i, x)\Big)\, \chi(A, \mathfrak{R}, x).$$

Die Abbildungsfunktion $\chi(A, \mathfrak{R}, x)$ ist somit durch die Eigenschaften, multiplikativ zu sein, zum Annihilator von $(A, \mathfrak{R})$ zu gehören und dabei den niedrigst möglichen Grad $n(A, \mathfrak{R}) = \dim \mathfrak{R}$ zu besitzen, eindeutig bestimmt. $\chi(A, \mathfrak{R}, x)$ heiße „charakteristisches Polynom" von $(A, \mathfrak{R})$. Es sei für später hervorgehoben, daß im Falle eines zyklischen $(A, \mathfrak{R})$, bei welchem das Minimalpolynom von $(A, \mathfrak{R})$ selber den Grad $\dim \mathfrak{R}$ hat, dieses nach II mit dem charakteristischen Polynom von $(A, \mathfrak{R})$ zusammenfällt.

4. Die konstanten Glieder der charakteristischen Polynome bilden die Werte einer Abbildungsfunktion $\Delta(A, \mathfrak{R}) = \chi(A, \mathfrak{R}, 0)$, die nach I multiplikativ ist, d. h. $\Delta(A, \mathfrak{R}) = \Delta(A_1, \mathfrak{R}_1)\, \Delta(A_2, \mathfrak{R}_2)$ erfüllt für jede Zerlegung $(A, \mathfrak{R}) = (A_1, \mathfrak{R}_1) + (A_2, \mathfrak{R}_2)$. Sie

hat zudem die wichtige Eigenschaft, daß aus ihr wieder das charakteristische Polynom gewonnen werden kann, indem nämlich

$$\Delta(A - \lambda E, \mathfrak{R}) = \chi(A, \mathfrak{R}, \lambda) \quad \text{für alle } \lambda \in K \tag{4.1}$$

gilt (E = identische Abbildung auf $\mathfrak{R}$). Es werde gleich die etwas allgemeinere Beziehung bewiesen:

$$\chi(A - \lambda E, \mathfrak{R}, x) = \chi(A, \mathfrak{R}, x + \lambda).$$

Sei $\varphi(x)$ ein Polynom aus $K[x]$; definiert man für ein $\lambda \in K$ das Polynom $\varphi_\lambda(x)$ durch $\varphi_\lambda(x) = \varphi(x + \lambda)$, so gilt, wie unmittelbar nachzuprüfen, für jede Abbildung $(A, \mathfrak{R})$ stets $\varphi_\lambda(A - \lambda E) = \varphi(A)$. Daraus folgert man mühelos die Beziehung $\mu(A - \lambda E, \mathfrak{R}, x) = \mu(A, \mathfrak{R}, x + \lambda)$. Weiter liefert jede vollständige Zerlegung $(A, \mathfrak{R}) = \sum\limits_1^m (A_i, \mathfrak{R}_i)$ auch eine vollständige Zerlegung $(A - \lambda E, \mathfrak{R}) = \sum\limits_1^m (A_i - \lambda E_i, \mathfrak{R}_i)$ (E_i = identische Abbildung auf $\mathfrak{R}_i$). Daher ist nach 3.

$$\chi(A - \lambda E, \mathfrak{R}, x) = \prod_1^m \mu(A_i - \lambda E_i, \mathfrak{R}_i, x) = \prod_1^m \mu(A_i, \mathfrak{R}_i, x + \lambda) = \chi(A, \mathfrak{R}, x + \lambda).$$

Die Funktion $\Delta(A, \mathfrak{R})$ ist natürlich durch die Eigenschaft (4.1) vollständig charakterisiert. Man bezeichnet aus Normierungsgründen (wegen $\Delta(E, \mathfrak{R}) = (-1)^n$, $n = \dim \mathfrak{R}$, und wegen des unten zu beweisenden Multiplikationssatzes) nicht $\Delta(A, \mathfrak{R})$, sondern $(-1)^n \Delta(A, \mathfrak{R})$ als „Determinante von $(A, \mathfrak{R})$".

Ganz analog kann man die negativen Koeffizienten der zweithöchsten Glieder der charakteristischen Polynome als Werte einer Abbildungsfunktion $\sigma(A, \mathfrak{R})$ wählen, also $\chi(A, \mathfrak{R}, x) = x^n - \sigma(A, \mathfrak{R})\, x^{n-1} + \dots$. Diese Funktion ist „additiv", d. h. es gilt $\sigma(A, \mathfrak{R}) = \sigma(A_1, \mathfrak{R}_1) + \sigma(A_2, \mathfrak{R}_2)$ für jede Zerlegung $(A, \mathfrak{R}) = (A_1, \mathfrak{R}_1) + (A_2, \mathfrak{R}_2)$. $\sigma(A, \mathfrak{R})$ ist die „Spur von $(A, \mathfrak{R})$".

5. Die wichtigsten elementaren Eigenschaften von charakteristischem Polynom, Determinante und Spur (vgl. etwa [2a], §§ 39, 40) können nun auf dem bei ihrer Definition beschrittenen Weg bewiesen werden. Seien zuerst A und A^* ähnliche Abbildungen eines Vektorraums $\mathfrak{R}$ in sich, d. h. es existiere eine reguläre (1—1-deutige) Abbildung X auf $\mathfrak{R}$ so, daß $A^* = X^{-1} A X$. Dann sind die charakteristischen Polynome (und damit natürlich auch die Determinanten und die Spuren) von A und A^* gleich. Jede vollständige Zerlegung von $(A, \mathfrak{R})$ liefert nämlich auch eine solche von $(A^*, \mathfrak{R})$ und umgekehrt; die bei diesen Zerlegungen auftretenden, einander entsprechenden Minimalpolynome sind aber schon gleich, wie sofort festzustellen. Die Behauptung folgt dann nach 2. Aus ihr läßt sich auch die Gleichheit der charakteristischen Polynome einer Abbildung und der zu ihr transponierten im Dualraum ableiten. Man hat es nur nötig, eine isomorphe Beziehung des Dualraums zum ursprünglichen Raum herzustellen, wodurch die transponierte der gegebenen Abbildung in eine zu dieser ähnlichen übergehen wird.

Man erkennt weiter leicht, daß eine Abbildung $(A, \mathfrak{R})$ dann und nur dann singulär (nicht 1—1-deutig) ist, wenn $\Delta(A, \mathfrak{R}) = 0$ ausfällt. Ist nämlich $\Delta(A, \mathfrak{R}) = \chi(A, \mathfrak{R}, 0) = 0$, so muß mindestens eines der nach 2. das Polynom $\chi(A, \mathfrak{R}, x)$ bildenden Minimal-

polynome ein verschwindendes konstantes Glied haben; hieraus folgt die Singularität von $(A, \mathfrak{R})$ ohne weiteres. Ist umgekehrt $(A, \mathfrak{R})$ singulär, so gibt es einen Vektor $a \in \mathfrak{R}$ mit $a \neq 0$, $Aa = 0$, dessen Ordnungspolynom bzgl. A somit $\omega(x) = x$ lautet. Dann ist aber das Minimalpolynom und damit auch das charakteristische Polynom von $(A, \mathfrak{R})$ durch x teilbar, wie behauptet. Zusammen mit (4.1) liefert dieses Ergebnis weiter die Tatsache, daß ein Eigenvektor $e \neq 0$ einer Abbildung $(A, \mathfrak{R})$ mit $Ae = \lambda e$ dann und nur dann existiert, wenn $\chi(A, \mathfrak{R}, \lambda) = 0$ ist.

Eine bequeme Eigenschaft des charakteristischen Polynoms ist auch seine Unveränderlichkeit beim Übergang zu einem Erweiterungskörper K^* des Grundkörpers K und entsprechender Erweiterung der Abbildungen $(A, \mathfrak{R})$ zu $(A^*, \mathfrak{R}^*)$ (vgl. etwa [3], VII, § 8). Identifiziert man $\mathfrak{R}$ mit einer Teilmenge von $\mathfrak{R}^*$, so bleibt die lineare Unabhängigkeit bzgl. K von Vektoren aus $\mathfrak{R}$ auch bzgl. K^* bestehen. Daraus folgt unmittelbar die Invarianz der Ordnungspolynome der Vektoren von $\mathfrak{R}$ und damit auch die des Minimalpolynoms beim Übergang zu K^*. Jede vollständige Zerlegung $(A, \mathfrak{R}) = \sum (A_i, \mathfrak{R}_i)$ erzeugt auch eine Zerlegung $(A^*, \mathfrak{R}^*) = \sum (A_i^*, \mathfrak{R}_i^*)$ und man folgert wieder aus der Erhaltung der linearen Unabhängigkeit, daß jedes $(A_i^*, \mathfrak{R}_i^*)$ zyklisch ist. Dadurch wird $\chi(A_i^*, \mathfrak{R}_i^*, x) = \mu(A_i^*, \mathfrak{R}_i^*, x)$; dieses letztere Polynom ist aber nach der obigen Bemerkung seinerseits gleich $\mu(A_i, \mathfrak{R}_i, x) = \chi(A_i, \mathfrak{R}_i, x)$. Daher ist $\chi(A^*, \mathfrak{R}^*, x) = \chi(A, \mathfrak{R}, x)$ nach I. (Unter Umständen ist wegen der nur bis auf eine Isomorphie bestimmten Erweiterung auch noch die Ähnlichkeitsinvarianz von χ zu berücksichtigen.)

6. Etwas tiefer liegt eine Beziehung für charakteristische Polynome, die eine gewisse Verallgemeinerung der Multiplikativität I darstellt. Sei $\mathfrak{U} \subset \mathfrak{R}$ ein bei der Abbildung $(A, \mathfrak{R})$ invarianter Unterraum und $\mathfrak{R}/\mathfrak{U}$ der von ihm gebildete Faktorraum; mit $(U, \mathfrak{U})$ bzw. $(V, \mathfrak{R}/\mathfrak{U})$ mögen die von A auf $\mathfrak{U}$ bzw. $\mathfrak{R}/\mathfrak{U}$ (kanonisch) induzierten Abbildungen bezeichnet werden. Dann gilt:

(6.1) $$\chi(A, \mathfrak{R}, x) = \chi(U, \mathfrak{U}, x)\, \chi(V, \mathfrak{R}/\mathfrak{U}, x),$$

sowie, daraus folgend,

(6.2) $$\Delta(A, \mathfrak{R}) = \Delta(U, \mathfrak{U})\, \Delta(V, \mathfrak{R}/\mathfrak{U}); \quad \sigma(A, \mathfrak{R}) = \sigma(U, \mathfrak{U}) + \sigma(V, \mathfrak{R}/\mathfrak{U}).$$

Die Formel (6.1) werde zuerst für Abbildungen $(A, \mathfrak{R})$ mit $\mu(A, \mathfrak{R}, x) = \pi(x)^r$, $\pi(x)$ irreduzibel in $K[x]$ (etwa vom Grade p), bewiesen. Nach den Ausführungen von 2. und 3. ist in diesem Falle $\chi(A, \mathfrak{R}, x) = \pi(x)^k$ und $\chi(U, \mathfrak{U}, x) = \pi(x)^m$ mit $pk = \dim \mathfrak{R}$, $pm = \dim \mathfrak{U}$. Analog erweist sich auch $\chi(V, \mathfrak{R}/\mathfrak{U}, x)$ als eine Potenz von $\pi(x)$, nämlich $\chi(V, \mathfrak{U}/\mathfrak{R}, x) = \pi(x)^q$ mit $pq = \dim \mathfrak{R}/\mathfrak{U} = \dim \mathfrak{R} - \dim \mathfrak{U}$. Damit ist (6.1) in diesem Falle bestätigt.

Zum Nachweis des allgemeinen Falles sei (mit angepaßten Bezeichnungen) $(A, \mathfrak{R}) = \sum_1^s (A_i, \mathfrak{R}_i)$ die primäre Zerlegung von $(A, \mathfrak{R})$ und $(U, \mathfrak{U}) = \sum_1^r (U_i, \mathfrak{U}_i)$ diejenige von $(U, \mathfrak{U})$. Es ist $r \leqq s$ und es kann die Bezeichnung so gewählt werden, daß $\mathfrak{U}_i \subset \mathfrak{R}_i$ für $i = 1, \ldots, r$; für $i = r + 1, \ldots, s$ wird, wenn nötig, einfach $\mathfrak{U}_i = 0$ gesetzt. Nach dem

im vorhergehenden Absatz bewiesenen Sachverhalt ist sicherlich $\chi(A_i, \mathfrak{R}_i, x) = \chi(U_i, \mathfrak{U}_i, x)\, \chi(V_i, \mathfrak{R}_i/\mathfrak{U}_i, x)$. Nun lassen sich aber der Vektorraum $\mathfrak{R}/\mathfrak{U} = \sum_1^s \mathfrak{R}_i / \sum_1^s \mathfrak{U}_i$ und der Produktraum $\prod_1^s \mathfrak{R}_i/\mathfrak{U}_i$ so isomorph aufeinander beziehen, daß die von A auf $\prod_1^s \mathfrak{R}_i/\mathfrak{U}_i$ kanonisch induzierte Abbildung in die Abbildung V auf $\mathfrak{R}/\mathfrak{U}$ übergeht. Nach I ist daher $\chi(V, \mathfrak{R}/\mathfrak{U}, x) = \prod_1^s \chi(V_i, \mathfrak{R}_i/\mathfrak{U}_i, x)$; zusammen mit den soeben abgeleiteten Formeln ergibt sich wieder (6.1).

Als Anwendung kann die Gleichung $\chi(AB, \mathfrak{R}, x) = \chi(BA, \mathfrak{R}, x)$ auf einem dem Beweis mit Matrizen ähnlichen Weg abgeleitet werden (vgl. [2b], § 53, Ex. 13 und § 51). Es genügt einmal, die Gleichung für den Fall zu bestätigen, daß A gleich einer Projektion P ist. Im Falle eines beliebigen $(A, \mathfrak{R})$ kann man dann nämlich stets eine reguläre Abbildung $(X, \mathfrak{R})$ so finden, daß XA einer Projektion gleich wird. Dann ist einmal $\chi(XABX^{-1}, \mathfrak{R}, x) = \chi(BA, \mathfrak{R}, x)$, andererseits nach 5. auch

$$\chi(XABX^{-1}, \mathfrak{R}, x) = \chi(AB, \mathfrak{R}, x).$$

Sei also $A = P$ eine Projektion längs $\mathfrak{B}$ auf $\mathfrak{U}$ ($\mathfrak{U}$ und $\mathfrak{B}$ komplementäre Unterräume von $\mathfrak{R}$, $\dim \mathfrak{B} = k$), und B eine beliebige andere Abbildung auf $\mathfrak{R}$. Es ist klar, daß $\mathfrak{U}$ bei PB invariant bleibt und daß PB auf dem k-dimensionalen Faktorraum $\mathfrak{R}/\mathfrak{U}$ die Nullabbildung erzeugt. Es ist daher nach (6.1) (der Einfachheit halber werden im folgenden induzierte Abbildungen mit denselben Buchstaben bezeichnet wie die induzierenden): $\chi(PB, \mathfrak{R}/\mathfrak{U}, x) = x^k$, $\chi(PB, \mathfrak{R}, x) = x^k \chi(PB, \mathfrak{U}, x)$. Andererseits erzeugt BP auf $\mathfrak{B}$ die Nullabbildung, so daß analog: $\chi(BP, \mathfrak{B}, x) = x^k$, $\chi(BP, \mathfrak{R}, x) = x^k \chi(BP, \mathfrak{R}/\mathfrak{B}, x)$. Wie man sich leicht überzeugt, führt aber die kanonisch isomorphe Beziehung von $\mathfrak{U}$ und $\mathfrak{R}/\mathfrak{B}$ die beiden Abbildungen $(PB, \mathfrak{U})$ und $(BP, \mathfrak{R}/\mathfrak{B})$ ineinander über, so daß $\chi(PB, \mathfrak{U}, x) = \chi(BP, \mathfrak{R}/\mathfrak{B}, x)$. Damit ist der Beweis vollständig.

7. Die beiden abschließenden Sätze, der Multiplikationssatz für Determinanten und der Additionssatz für Spuren, benötigen zwei Hilfssätze. Zu deren Vorbereitung werde ein Vektorraum $\mathfrak{R}$ der Dimension $n + 2$ $(n \geqq 0)$ betrachtet, auf dem die Vektoren $(d, e, e_1, \ldots, e_n)$ eine Basis bilden mögen. Eine Abbildung $(U, \mathfrak{R})$ erfülle $Ud = e$ und es werde weiter gesetzt $Ue = f$, $Ue_i = f_i$, so daß insgesamt

$$Ud = e, \quad Ue = f, \quad Ue_i = f_i \quad (i = 1, \ldots, n).$$

Die Vektoren $d, Ud, U^2 d, \ldots$ spannen einen Unterraum $\mathfrak{D} \subset \mathfrak{R}$ auf, auf dem $(U, \mathfrak{D})$ zyklisch ist. Für $\mathfrak{D}$ (das natürlich mit $\mathfrak{R}$ zusammenfallen kann) werde im folgenden die Basis $(d, Ud, U^2 d, \ldots, U^{m-1} d)$ gewählt. Endlich sei $\chi(U, \mathfrak{D}, x) = \delta_0 + \delta_1 x + \cdots + \delta_{m-1} x^{m-1} + x^m$. Unter Verwendung dieser Bezeichnungen gelten:

Hilfssatz 1. *Ist* $(V, \mathfrak{R})$ *eine Abbildung mit*

$$Vd = (1/\lambda) f, \quad Ve = \lambda e, \quad Ve_i = f_i \quad (i = 1, \ldots, n; \lambda \neq 0),$$

so ist $\Delta(V, \mathfrak{R}) = -\Delta(U, \mathfrak{R})$.

Hilfssatz 2. *Ist* $(W, \mathfrak{R})$ *eine Abbildung mit*

$$Wd = \mu d, \quad We = f - \mu e + \nu d, \quad We_i = f_i \quad (i = 1, \ldots, n),$$

so ist $\sigma(W, \mathfrak{R}) = \sigma(U, \mathfrak{R})$.

Beweis von Hilfssatz 1. Für jeden Vektor $r \in \mathfrak{R}$ gilt mit geeigneten $\varrho, \sigma \in K$:

$$Vr - Ur = \varrho e + \sigma f, \tag{7.1}$$

wie unmittelbar nachzuprüfen. Hieraus und aus $U^2 d = \lambda V d$ folgt durch sukzessive Anwendung von U auf d die Richtigkeit der folgenden, mit bestimmten Koeffizienten ϱ versehenen Beziehungen

$$U^i d = \lambda V^{i-1} d + \varrho_{i,i-2} V^{i-2} d + \cdots + \varrho_{i1} V d + \varrho_i e \quad (i \geqq 2). \tag{7.2}$$

Aus (7.1) und $e = Ud$, $f = U^2 d \in \mathfrak{D}$ ergibt sich die Invarianz von $\mathfrak{D}$ bei V und aus $Ve = \lambda e$ folgt, mit $\mathfrak{E} = (e)$, auch diejenige von $\mathfrak{D}/\mathfrak{E}$; die von V induzierten Abbildungen mögen wieder mit $(V, \mathfrak{D})$ bzw. $(V, \mathfrak{D}/\mathfrak{E})$ bezeichnet werden. Man stellt nun fest, daß $(V, \mathfrak{D}/\mathfrak{E})$ bzgl. der zu d gehörigen Restklasse $d^* \in \mathfrak{D}/\mathfrak{E}$ zyklisch ist; man hat zu diesem Zweck nur die Vektoren von $\mathfrak{D}$ in der oben gewählten Basis darzustellen und die auftretenden Ausdrücke $U^i d$ gemäß (7.2) zu ersetzen.

Nach II gilt sicher $\chi(U, \mathfrak{D}, U) d = 0$. Substituiert man in dieser Gleichung für Ud den Vektor e und für die $U^i d$ $(i \geqq 2)$ die Ausdrücke (7.2), so erhält man eine Beziehung der Form $\delta_0 d + \varepsilon_1 V d + \cdots + \varepsilon_{m-2} V^{m-2} d + \lambda V^{m-1} d + \varepsilon_m e = 0$ mit bestimmten Koeffizienten ε; sie besagt offenbar, daß das Polynom $\varepsilon(x) = \delta_0 + \varepsilon_1 x + \cdots + \varepsilon_{m-2} x^{m-2} + \lambda x^{m-1}$ ein Vielfaches des Ordnungspolynoms von d^*, des erzeugenden Vektors von $(V, \mathfrak{D}/\mathfrak{E})$, ist. Da $(V, \mathfrak{D}/\mathfrak{E})$ als zyklisch erkannt wurde und $\mathfrak{D}/\mathfrak{E}$ die Dimension $m-1$ hat, muß $(1/\lambda)\, \varepsilon(x) = \mu(V, \mathfrak{D}/\mathfrak{E}, x) = \chi(V, \mathfrak{D}/\mathfrak{E}, x)$, also $\Delta(V, \mathfrak{D}/\mathfrak{E}) = \delta_0/\lambda$ sein. Aus $Ve = \lambda e$ und (6.2) folgt dann $\Delta(V, \mathfrak{D}) = -\delta_0$ und wegen $\delta_0 = \Delta(U, \mathfrak{D})$ schließlich $\Delta(V, \mathfrak{D}) = -\Delta(U, \mathfrak{D})$.

Ist $\mathfrak{D} = \mathfrak{R}$, so ist damit Hilfssatz 1 bewiesen. Andernfalls betrachte man den Faktorraum $\mathfrak{R}/\mathfrak{D}$; da U und V nach (7.1) auf ihm dieselben Abbildungen induzieren, folgt Hilfssatz 1 wieder aus (6.2).

Der Beweis von Hilfssatz 2 folgt denselben Richtlinien wie der soeben erbrachte von Hilfssatz 1. Man erhält analog zu (7.1) und (7.2) für U und W die Beziehungen:

$$Wr - Ur = \varrho' d + \sigma' e \quad (r \in \mathfrak{R}), \tag{7.3}$$

$$U^i d = W^{i-1} e + \mu W^{i-2} e + \varrho'_{i,i-3} W^{i-3} e + \cdots + \varrho'_{i1} We + \varrho'_{i0} e + \varrho'_i d \quad (i \geqq 2). \tag{7.4}$$

Aus (7.3) folgt wieder die Invarianz des Unterraums $\mathfrak{D}$ bei der Abbildung W und damit auch, falls $\mathfrak{D}^* = (d)$ gesetzt wird, die des Faktorraums $\mathfrak{D}/\mathfrak{D}^*$; (7.4) ergibt, daß $(W, \mathfrak{D}/\mathfrak{D}^*)$ zyklisch ist bzgl. der zum Vektor e gehörenden Restklasse $e^* \in \mathfrak{D}/\mathfrak{D}^*$. Ersetzt man schließlich in der Gleichung $\chi(U, \mathfrak{D}, U) d = 0$ wieder Ud durch e und die $U^i d$ $(i \geqq 2)$ gemäß (7.4), so erhält man

$$\varepsilon'_0 e + \varepsilon'_1 We + \cdots + \varepsilon'_{m-3} W^{m-3} e + (\delta_{m-1} + \mu) W^{m-2} e + W^{m-1} e + \varepsilon'_m d = 0$$

mit bestimmten ε', woraus sich wie oben

$$\chi(W, \mathfrak{D}/\mathfrak{D}^*, x) = \varepsilon_0' + \varepsilon_1' x + \cdots + \varepsilon_{m-3}' x^{m-3} + (\delta_{m-1} + \mu) x^{m-2} + x^{m-1}$$

ergibt. Es ist also $\sigma(W, \mathfrak{D}/\mathfrak{D}^*) = -(\delta_{m-1} + \mu)$; zusammen mit $Wd = \mu d$, (6.2) und $\sigma(U, \mathfrak{D}) = -\delta_{m-1}$ folgt hieraus $\sigma(W, \mathfrak{D}) = \sigma(U, \mathfrak{D})$. Der Schluß des Beweises verläuft wie bei Hilfssatz 1.

8. Es seien nun A und B zwei lineare Abbildungen desselben Vektorraums $\mathfrak{R}$ in sich und BA ihr Produkt. Der Multiplikationssatz für die Determinanten ist selbstverständlich im Falle der Singularität einer der beiden Abbildungen sowie im Falle $\dim \mathfrak{R} = 1$. Es werde daher angenommen, daß $\dim \mathfrak{R} = n + 2$ $(n \geqq 0)$, und daß A und B regulär seien. Weiter kann vorausgesetzt werden, daß BA einen Eigenvektor $e \neq 0$ mit $BAe = \lambda e$ besitzt. Ist das nämlich nicht der Fall, so adjungiere man zum Grundkörper K eine Wurzel des charakteristischen Polynoms $\chi(BA, \mathfrak{R}, x)$ und gehe zum Erweiterungskörper $K^* = K(\lambda)$ über, was im Lichte der Ausführungen von 5. gestattet ist.

Besitzt A ebenfalls den Eigenvektor e, so gilt dasselbe von B und der Beweis des Multiplikationssatzes kann, wie weiter unten angegeben, fortgesetzt werden. Andernfalls wird der Vektor $d \in \mathfrak{R}$, für welchen $Ad = e$ ist, von e linear unabhängig sein; dann ergänze man, wenn nötig, die beiden Vektoren d, e durch $e_1, e_2, \ldots, e_n$ zu einer vollen Basis von $\mathfrak{R}$. A und B mögen dabei lauten:

$$Ad = e,\quad Ae = f,\quad Ae_i = f_i;\quad Be = d',\quad Bf = \lambda e,\quad Bf_i = e_i' \quad (i = 1, \ldots, n).$$

Nun werden A und B durch die folgenden beiden Abbildungen U, V auf $\mathfrak{R}$ ersetzt:

$$Ud = f,\quad Ue = e,\quad Ue_i = f_i;\quad Vf = d',\quad Ve = \lambda e,\quad Vf_i = e_i' \quad (i = 1, \ldots, n).$$

Man bemerkt, daß $VU = BA$ gilt und daß U zu A bzw. V zu B in der durch den Hilfssatz 1 beschriebenen Beziehung stehen, daß ihre Determinanten also je bis auf das Vorzeichen übereinstimmen. Alle drei Abbildungen U, V, VU lassen jetzt den von e erzeugten 1-dimensionalen Unterraum $\mathfrak{E} \subset \mathfrak{R}$ invariant. Bei Betrachtung des Faktorraums $\mathfrak{R}/\mathfrak{E}$ und Anwendung von Formel (6.2) folgt nun unmittelbar der Beweis des Multiplikationssatzes durch vollständige Induktion nach der Dimensionszahl des Raumes.

Der Beweis des Additionsgesetzes für die Spuren verläuft analog. Bei gegebenen Abbildungen A und B auf $\mathfrak{R}$ kann man wieder, neben $\dim \mathfrak{R} \geqq 2$, annehmen, daß $A + B$ einen Eigenvektor $d \neq 0$ mit $(A + B)d = (\mu + 1)d$ besitzt. Ist d auch Eigenvektor von A, so ist er es auch von B und man kommt wieder direkt mit vollständiger Induktion zum Ziel. Andernfalls wird der Vektor $e = Ad$ von d linear unabhängig sein; nach Ergänzung zu einer Basis $(d, e, e_1, \ldots, e_n)$ von $\mathfrak{R}$ mögen dann A und B die Gestalt haben:

$$Ad = e,\quad Ae = f,\quad Ae_i = f_i;\quad Bd = (\mu + 1)d - e,\quad Be = f',\quad Be_i = f_i' \quad (i = 1, \ldots, n).$$

Man ersetze hierauf A und B durch die folgenden beiden Abbildungen U und V:

$$Ud = d,\quad Ue = f - e,\quad Ue_i = f_i;\quad Vd = \mu d,\quad Ve = f' + e,\quad Ve_i = f_i' \quad (i = 1, \ldots, n).$$

Man erkennt wieder, daß einerseits $U + V = A + B$, und daß andererseits U zu A bzw. V zu B in derselben Beziehung zueinander stehen wie die beiden in Hilfssatz 2

betrachteten Abbildungen, so daß ihre Spuren je gleich werden. Wegen der Invarianz des von d erzeugten Unterraums bei U, V und $U + V$ führt nach (6.2) wiederum vollständige Induktion nach der Dimensionszahl des Raumes zum Ziel.

9. Es bleibt noch zu zeigen, daß die in 3. und 4. erklärten Abbildungsfunktionen charakteristisches Polynom, Determinante und Spur mit den auf eine der in 1. erwähnten Arten gewonnenen Funktionen übereinstimmen. Dies läuft nach Satz 2 darauf hinaus, zu beweisen, daß die Polynome n-ten Grades $\varkappa(A, \mathfrak{R}, \lambda) = (-1)^n |A - \lambda E|$ ($n = \dim \mathfrak{R}$) als Funktionen von $(A, \mathfrak{R})$ multiplikativ sind und zum Annihilator von $(A, \mathfrak{R})$ gehören. Dies ist aber eine Folge des Entwicklungssatzes für Determinanten von Laplace und des Satzes von Hamilton-Cayley.

Literaturverzeichnis

[1] A. Bergmann, Ein Axiomensystem für Determinanten. Arch. Math. **10**, 243–256 (1959).
[2a] P. R. Halmos, Finite Dimensional Vector Spaces. Annals of Math. Studies Nr. 7, Princeton 1942.
[2b] P. R. Halmos, Finite Dimensional Vector Spaces. 2nd ed. D. Van Nostrand Co. Inc. 1958.
[3] N. Jacobson, Lectures in Abstract Algebra, Vol. II. D. Van Nostrand Co. Inc. 1958.
[4] G. Pickert, Lineare Algebra. Enzykl. math. Wiss. 2. Aufl., Band I, 1, 6. 1953.
[5] P. Wilker, Rekursive Definition der Determinante. Elemente Math. **14**, 63–64 (1959).

Eingegangen am 19. 8. 1960

Anschrift des Autors:
Peter Wilker
Bern-Liebefeld, Schweiz
Buchenweg 18

On the Components of Ideals in Commutative Rings

By

BERNHARD BANASCHEWSKI

Introduction. In the theory of decomposable ideals of a commutative ring $\mathfrak{o}$ one has the following propositions concerning the relation between the prime ideals belonging to an ideal $\mathfrak{a}$ and the components $\mathfrak{a}_S$ of $\mathfrak{a}$ with respect to multiplicatively closed sets $S \subseteqq \mathfrak{o}$:

I. *The prime ideals belonging to $\mathfrak{a}_S$ are exactly the prime ideals $\mathfrak{p}$ belonging to $\mathfrak{a}$ such that $S \cap \mathfrak{p} = \varnothing$.*

II. *If two multiplicatively closed sets $S, T \subseteqq \mathfrak{o}$ meet exactly the same prime ideals belonging to $\mathfrak{a}$ then $\mathfrak{a}_S = a_T$.*

III. *For any isolated set $\mathscr{X}$ of prime ideals belonging to $\mathfrak{a}$ there exists a component $\mathfrak{a}_S$ of $\mathfrak{a}$ such that $\mathscr{X}$ is the set of all prime ideals belonging to $\mathfrak{a}_S$.*

Here, the prime ideals belonging to a decomposable ideal $\mathfrak{a}$ may be taken as the radicals of those primary ideals which occur in some irredundant primary decomposition of $\mathfrak{a}$. In [2] KRULL associated with *any* ideal $\mathfrak{a}$ of a commutative ring $\mathfrak{o}$ a particular set of prime ideals which turned out to be precisely the set of prime ideals belonging to $\mathfrak{a}$ if $\mathfrak{a}$ is decomposable, and which was therefore also called the set of prime ideals belonging to $\mathfrak{a}$. With this concept thus extended to arbitrary ideals, the question was raised in [2] whether the above propositions still hold if $\mathfrak{a}$ is arbitrary and not merely decomposable. More precisely, the question was whether I and II are generally satisfied and whether there is a suitable reformulation of III which holds in the general case (the latter because there are examples for which III, as it stands, is actually false). This problem has so far remained unsolved. KRULL himself remarked in [2] that on the basis of a certain conjecture (namely, that for any ideal $\mathfrak{a}$ in any ring $\mathfrak{o}$ the relatively maximal prime ideals of $\mathfrak{a}$ belong to $\mathfrak{a}$) I and II hold in general. However, the status of this conjecture is still unsettled.

In a recent paper on the ideal theory of some very special rings [1], the propositions I and II were proved for the ideals of those rings without dealing with KRULL's conjecture at all, and it was thereby suggested thad these propositions might be proved for arbitrary rings in a similar way. This turned out to be the case, and the present paper is concerned with this matter. Moreover, it is shown here that III becomes a general theorem if the term "isolated" is replaced by "closed", a subset $\mathscr{X}$ of a set $\mathscr{E}$ of primes being called closed (in $\mathscr{E}$) if and only if $\mathfrak{p} \subseteqq \bigcup \mathfrak{r} (\mathfrak{r} \in \mathscr{X})$, $\mathfrak{p} \in \mathscr{E}$, implies $\mathfrak{p} \in \mathscr{X}$.

Since the closed subsets of a *finite* $\mathscr{E}$ are precisely the isolated subsets of $\mathscr{E}$ this new proposition amounts to the same as III if the ideal $\mathfrak{a}$ is decomposable[1]).

1. Extremal multiplicatively closed sets. For the time being it will be assumed that the commutative ring $\mathfrak{o}$ under consideration possesses a unit element 1. At some later stage, it will be indicated how the results proved under this restriction can also be obtained in the absence of a unit element. The ideals of $\mathfrak{o}$ will be denoted by $\mathfrak{a}, \ldots, \mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots$, the multiplicatively closed subsets of $\mathfrak{o}$ by $S, T, R, \ldots$ and the component of an ideal $\mathfrak{a}$ with respect to a multiplicatively closed set $S \subseteqq \mathfrak{o}$ by $\mathfrak{a}_S$. Furthermore, a prime or primary ideal is always taken to be proper and a multiplicatively closed set to be non-void. These latter conventions, incidentally, will have to be changed when rings without a unit element are discussed.

Concerning the components of an ideal $\mathfrak{a}$ one has the following basic rules:

Lemma 1. (i) $\mathfrak{a} \subseteqq \mathfrak{a}_S$. (ii) *If* $S \subseteqq T$ *then* $\mathfrak{a}_S \subseteqq \mathfrak{a}_T$. (iii) $(\mathfrak{a}_T)_S = \mathfrak{a}_{ST}$. (iv) $(\mathfrak{a}_S)_S = \mathfrak{a}_S$. (v) *If* $S \subseteqq T$ *then* $(\mathfrak{a}_S)_T = \mathfrak{a}_T$.

Proof. Of these statements, (i) and (ii) are obvious whilst (iv) and (v) follow directly from the preceding ones. To prove the remaining (iii), let first $\xi \in (\mathfrak{a}_T)_S$. Then, $\xi\alpha \in \mathfrak{a}_T$ with some $\alpha \in S$ and thus $\xi\alpha\beta \in \mathfrak{a}$ with some $\alpha\beta \in ST$. Conversely, if $\xi \in \mathfrak{a}_{ST}$, i.e., $\xi\alpha\beta \in \mathfrak{a}$ with some $\alpha \in S$ and $\beta \in T$, one has $\xi\alpha \in \mathfrak{a}_T$ and hence $\xi \in (\mathfrak{a}_T)_S$.

An identity for the components of certain quotients is given in

Lemma 2. *For any* $\gamma \in \mathfrak{o}$, $(\mathfrak{a} : (\gamma))_S = \mathfrak{a}_S : (\gamma)$.

Proof. $\xi \in (\mathfrak{a} : (\gamma))_S$ means that $\xi\alpha \in \mathfrak{a} : (\gamma)$ for some $\alpha \in S$ and hence $\xi\alpha\gamma \in \mathfrak{a}$ for some $\alpha \in S$ which in turn means that $\xi\gamma \in \mathfrak{a}_S$, i.e., $\xi \in \mathfrak{a}_S : (\gamma)$.

The study of the set of all components of an ideal $\mathfrak{a}$ is greatly facilitated by singling out certain multiplicatively closed sets S in relation to $\mathfrak{a}$ in the following manner:

Definition. *S is called $\mathfrak{a}$-extremal iff $T \supset S$ implies $\mathfrak{a}_T \supset \mathfrak{a}_S$.*

It may be remarked that if $\mathfrak{a}_S = \mathfrak{o}$ (which is the case iff $S \cap \mathfrak{a} \neq \emptyset$) and $S \neq \mathfrak{o}$ then S is not $\mathfrak{a}$-extremal whereas $\mathfrak{o}$ is $\mathfrak{a}$-extremal since the condition defining $\mathfrak{a}$-extremality holds trivially for $S = \mathfrak{o}$. The existence of other $\mathfrak{a}$-extremal multiplicatively closed sets will soon become obvious.

An alternative description of $\mathfrak{a}$-extremality is given by

Lemma 3. *S is $\mathfrak{a}$-extremal iff $\mathfrak{a}_T \subseteqq \mathfrak{a}_S$ implies $T \subseteqq S$.*

Proof. Let S be $\mathfrak{a}$-extremal and $\mathfrak{a}_T \subseteqq \mathfrak{a}_S$. Then, consider the multiplicatively closed set $R = S \cup T \cup ST$. Clearly, $\mathfrak{a}_S \subseteqq \mathfrak{a}_R$ since $S \subseteqq R$. On the other hand, if $\xi\alpha \in \mathfrak{a}$ with $\alpha \in R$ then $\alpha \in S$ and hence $\xi \in \mathfrak{a}_S$ or $\alpha \in T$ and thus $\xi \in \mathfrak{a}_T \subseteqq \mathfrak{a}_S$ or $\alpha = \beta\gamma$ with $\beta \in S$, $\gamma \in T$ and therefore $\xi \in \mathfrak{a}_{ST} = (\mathfrak{a}_T)_S \subseteqq (\mathfrak{a}_S)_S = \mathfrak{a}_S$. In all, one has $\mathfrak{a}_R \subseteqq \mathfrak{a}_S$ and finally $\mathfrak{a}_S = \mathfrak{a}_R$. Since S is $\mathfrak{a}$-extremal, $R \supset S$ is hereby excluded and one ends up with $R = S$ which gives $T \subseteqq S$. Conversely, let S satisfy the stated condition and assume $T \supset S$. Then either $\mathfrak{a}_T \supset \mathfrak{a}_S$ or $\mathfrak{a}_T = \mathfrak{a}_S$, and since the latter implies $T \subseteqq S$ it is excluded.

---

1) The main parts of this paper were written during my stay at Tulane University, 1959—1960.

As immediate consequences one obtains from Lemma 3:

Corollary 1. *The set $F(\mathfrak{a}) = \{\alpha \mid \xi\alpha \in \mathfrak{a} \Rightarrow \xi \in \mathfrak{a}\}$ of all $\alpha \in \mathfrak{o}$ prime to $\mathfrak{a}$ is the smallest $\mathfrak{a}$-extremal multiplicatively closed set.*

Proof. Clearly, $F(\mathfrak{a})$ is multiplicatively closed and $1 \in F(\mathfrak{a})$, hence $F(\mathfrak{a}) \neq \varnothing$. Moreover, $\mathfrak{a}_{F(\mathfrak{a})} = \mathfrak{a}$ by definition of $F(\mathfrak{a})$, and therefore $\mathfrak{a}_T \subseteqq \mathfrak{a}_{F(\mathfrak{a})}$ means $\mathfrak{a}_T = \mathfrak{a}$ which implies $T \subseteqq F(\mathfrak{a})$. By Lemma 3, $F(\mathfrak{a})$ is thus $\mathfrak{a}$-extremal. Again, by the same lemma, $\mathfrak{a} \subseteqq \mathfrak{a}_S$ implies $F(\mathfrak{a}) \subseteqq S$ for any $\mathfrak{a}$-extremal S.

Corollary 2. *The intersection of any collection of $\mathfrak{a}$-extremal multiplicatively closed sets is again such a set.*

Proof. Let $\mathscr{S}$ be the collection in question and $T = \bigcap S\,(S \in \mathscr{S})$. Then, for any R, $\mathfrak{a}_R \subseteqq \mathfrak{a}_T$ implies $\mathfrak{a}_R \subseteqq \mathfrak{a}_S$ and hence $R \subseteqq S$ for each $S \in \mathscr{S}$, i.e., $R \subseteqq T$.

Next it will be shown that extremality with respect to the components of an ideal is closely related to extremality with respect to the ideal itself:

Lemma 4. *T is $\mathfrak{a}_S$-extremal iff $T \supseteqq S$ and T is $\mathfrak{a}$-extremal.*

Proof. Let T be $\mathfrak{a}_S$-extremal. Then, $T \supseteqq F(\mathfrak{a}_S)$ and since $S \subseteqq F(\mathfrak{a}_S)$ by $(\mathfrak{a}_S)_S = \mathfrak{a}_S$ one has $S \subseteqq T$. Now, this implies $(\mathfrak{a}_S)_T = \mathfrak{a}_T$; hence if $\mathfrak{a}_R \subseteqq \mathfrak{a}_T$ then $(\mathfrak{a}_S)_R = \mathfrak{a}_{SR} = \mathfrak{a}_{RS} = (\mathfrak{a}_R)_S \subseteqq$ $\subseteqq (\mathfrak{a}_T)_S = (\mathfrak{a}_S)_T$ and thus $R \subseteqq T$. This proves T is $\mathfrak{a}$-extremal. Conversely, let $T \supseteqq S$ be $\mathfrak{a}$-extremal. As before, one has $\mathfrak{a}_T = (\mathfrak{a}_S)_T$, and if $(\mathfrak{a}_S)_R \subseteqq (\mathfrak{a}_S)_T$ for some R then $\mathfrak{a}_R \subseteqq (\mathfrak{a}_S)_R \subseteqq$ $\subseteqq (\mathfrak{a}_S)_T = \mathfrak{a}_T$ shows that $R \subseteqq T$; hence T is $\mathfrak{a}_S$-extremal.

The last two results now lead to a further criterion for $\mathfrak{a}$-extremality:

Lemma 5. *S is $\mathfrak{a}$-extremal iff $F(\mathfrak{a}_S) = S$.*

Proof. $F(\mathfrak{a}_S)$ is $\mathfrak{a}_S$-extremal, hence $\mathfrak{a}$-extremal and thus S is $\mathfrak{a}$-extremal if $S = F(\mathfrak{a}_S)$. Conversely, if S is $\mathfrak{a}$-extremal it is $\mathfrak{a}_S$-extremal and thus $F(\mathfrak{a}_S) \subseteqq S$ whilst $S \subseteqq F(\mathfrak{a}_S)$ anyway by $(\mathfrak{a}_S)_S = \mathfrak{a}_S$.

Corollary. *For any S, $F(\mathfrak{a}_S)$ is the smallest $\mathfrak{a}$-extremal multiplicatively closed set containing S and the only $\mathfrak{a}$-extremal T with $\mathfrak{a}_T = \mathfrak{a}_S$.*

The second corollary of Lemma 3 states that the collection of $\mathfrak{a}$-extremal multiplicatively closed sets is a closure system, contained in the closure system of all multiplicatively closed sets. The last corollary now identifies the closure operator defined on the latter closure system associated with the former as the mapping $S \to F(\mathfrak{a}_S)$.

The last of the present sequence of lemmas is concerned with certain ideal quotients; it will play a fundamental role in the proof of the central result of this paper.

Lemma 6. *If S is $\mathfrak{a}:(\gamma)$-extremal then S is also $\mathfrak{a}$-extremal.*

Proof. Let S be $\mathfrak{a}:(\gamma)$-extremal and assume $\mathfrak{a}_T \subseteqq \mathfrak{a}_S$. Then $\mathfrak{a}_T:(\gamma) \subseteqq \mathfrak{a}_S:(\gamma)$, hence by Lemma 2 $(\mathfrak{a}:(\gamma))_T \subseteqq (\mathfrak{a}:(\gamma))_S$ and thus $T \subseteqq S$. This proves that S is $\mathfrak{a}$-extremal.

2. Extremal prime ideals. The considerations of the preceding section will now be applied to prime ideals on the basis of the following

Definition. *A prime ideal $\mathfrak{p} \supseteqq \mathfrak{a}$ is called $\mathfrak{a}$-extremal iff its complement $\complement\mathfrak{p}$ is an $\mathfrak{a}$-extremal multiplicatively closed set.*

The set of all $\mathfrak{a}$-extremal prime ideals will be denoted by $\mathscr{E}(\mathfrak{a})$. A further characterization of $\mathscr{E}(\mathfrak{a})$ is given by

Lemma 7. *$\mathfrak{p} \in \mathscr{E}(\mathfrak{a})$ iff $\mathfrak{p} \supseteqq \mathfrak{a}$ and $F(\mathfrak{a}(\mathfrak{p})) = \mathbf{C}\mathfrak{p}$, where $\mathfrak{a}(\mathfrak{p}) = \mathfrak{a}_{\mathbf{C}\mathfrak{p}}$.*

This follows immediately from Lemma 5, and it shows that $\mathscr{E}(\mathfrak{a})$ is precisely the set of all those prime ideals which Krull [2] called „zu $\mathfrak{a}$ gehörig".

In the following, it will be of fundamental importance to know that $\mathscr{E}(\mathfrak{a})$ is non-void for any proper ideal $\mathfrak{a}$ (whilst, incidentally, $\mathscr{E}(\mathfrak{o})$ is void simply because there are no prime ideals $\mathfrak{p} \supseteqq \mathfrak{o}$ at all). In order to see this it should first be remarked that for any such $\mathfrak{a}$ there exist prime ideals $\mathfrak{p}$ which are *minimal above* $\mathfrak{a}$, a consequence of Zorn's Lemma and the fact that the intersection of a chain (i.e., set totally ordered by inclusion) of prime ideals is a prime ideal, the latter in turn following from the observation that the union of a chain of multiplicatively closed sets is multiplicatively closed. Now one has, as in [2]:

Lemma 8. *If $\mathfrak{p}$ is a prime ideal minimal above $\mathfrak{a}$ then $\mathfrak{p}$ is $\mathfrak{a}$-extremal.*

Proof. Take $S \supset \mathbf{C}\mathfrak{p}$ and suppose $\mathfrak{a} \cap S = \varnothing$. Then, let $\mathfrak{r}$ be maximal such that $\mathfrak{r} \supseteqq \mathfrak{a}$ and $\mathfrak{r} \cap S = \varnothing$. $\mathfrak{r}$ is prime and $\mathfrak{r} \cap \mathbf{C}\mathfrak{p} = \varnothing$, hence $\mathfrak{r} \subseteqq \mathfrak{p}$ and thus $\mathfrak{r} = \mathfrak{p}$. But now $\mathbf{C}\mathfrak{p} \subset S \subseteqq \mathbf{C}\mathfrak{r} = \mathbf{C}\mathfrak{p}$, a contradiction. It follows that $\mathfrak{a} \cap S \neq \varnothing$ and therefore $\mathfrak{a}_S = \mathfrak{o}$. Since $\mathfrak{p}$ is prime it is proper, and from $\mathfrak{a}(\mathfrak{p}) \subseteqq \mathfrak{p} \subset \mathfrak{o} = \mathfrak{a}_S$ one sees that $\mathfrak{p}$ is $\mathfrak{a}$-extremal.

It may be added to Lemma 8 that the $\mathfrak{a}$-extremal multiplicatively closed sets $\mathbf{C}\mathfrak{p}$, $\mathfrak{p}$ minimal above $\mathfrak{a}$, are exactly the maximal proper subsets of $\mathfrak{o}$ which are $\mathfrak{a}$-extremal multiplicatively closed: That each such $\mathbf{C}\mathfrak{p}$ has this property is contained in the above proof. Conversely, if S is such a set then $\mathfrak{a} \cap S = \varnothing$ and one may take an ideal $\mathfrak{p}$ maximal such that $\mathfrak{p} \cap S = \varnothing$. This being prime, there exists a prime ideal $\mathfrak{r} \subseteqq \mathfrak{p}$ minimal above $\mathfrak{a}$, and one has $\mathbf{C}\mathfrak{r} \supseteqq \mathbf{C}\mathfrak{p} \supseteqq S$. $\mathbf{C}\mathfrak{r}$ is $\mathfrak{a}$-extremal by Lemma 8 and, of course, proper; hence $S = \mathbf{C}\mathfrak{r}$ which was to be shown.

A further result concerning $\mathfrak{a}$-extremal prime ideals $\mathfrak{p}$, this time about the components $\mathfrak{a}(\mathfrak{p}) = \mathfrak{a}_{\mathbf{C}\mathfrak{p}}$, is:

Lemma 9. *For any $\gamma \notin \mathfrak{a}$ there exists a $\mathfrak{p} \in \mathscr{E}(\mathfrak{a})$ such that $\gamma \notin \mathfrak{a}(\mathfrak{p})$.*

Proof. If $\gamma \notin \mathfrak{a}$ then $\mathfrak{a}:(\gamma) \subset \mathfrak{o}$, and there exists a prime ideal $\mathfrak{p}$ minimal above $\mathfrak{a}:(\gamma)$. Then, $\mathfrak{p}$ is $\mathfrak{a}:(\gamma)$-extremal by Lemma 8 and hence also $\mathfrak{a}$-extremal by Lemma 6. Now one has, from the definition of components, $\mathfrak{a}(\mathfrak{p}) = \{\xi \mid \mathfrak{a}:(\xi) \nsubseteqq \mathfrak{p}\}$ which immediately shows that $\gamma \notin \mathfrak{a}(\mathfrak{p})$.

This last lemma is the key to the following basic intersection theorem:

Proposition 1. *For any ideal $\mathfrak{a}$, $\mathfrak{a} = \bigcap \mathfrak{a}(\mathfrak{p})$ $(\mathfrak{p} \in \mathscr{E}(\mathfrak{a}))$.*

Proof. One has $\mathfrak{a} \subseteqq \mathfrak{a}(\mathfrak{p})$ for all $\mathfrak{p} \in \mathscr{E}(\mathfrak{a})$ and Lemma 9 shows that $\gamma \notin \mathfrak{a}$ implies

$$\gamma \notin \bigcap \mathfrak{a}(\mathfrak{p}) \; (\mathfrak{p} \in \mathscr{E}(\mathfrak{a})).$$

Remark 1. In [2] it was shown that $\mathfrak{a} = \bigcap \mathfrak{a}(\mathfrak{r})$ where $\mathfrak{r}$ ranges over the ideals maximal such that $\mathfrak{r} \cap F(\mathfrak{a}) = \varnothing$, i.e., where $\mathfrak{a}(\mathfrak{r})$ are the Hauptkomponenten of $\mathfrak{a}$. This occurs here as a consequence of Proposition 1 since $\mathfrak{p} \cap F(\mathfrak{a}) = \varnothing$ for any $\mathfrak{p} \in \mathscr{E}(\mathfrak{a})$ by the corollary 1 of Lemma 3 and thus there exists an $\mathfrak{r} \supseteqq \mathfrak{p}$ maximal such that $\mathfrak{r} \cap F(\mathfrak{a}) = \varnothing$ for which one has $\mathfrak{a}(\mathfrak{r}) \subseteqq \mathfrak{a}(\mathfrak{p})$. It follows from this that Proposition 1 is an improvement of the intersection theorem of [2] in terms of Hauptkomponenten.

Remark 2. The main point in the proof of Lemma 9, and hence of Proposition 1, is to find a $\mathfrak{p} \supseteqq \mathfrak{a}:(\gamma)$ in $\mathscr{E}(\mathfrak{a})$ for any $\gamma \notin \mathfrak{a}$. Since $\mathscr{E}(\mathfrak{c}) \neq \varnothing$ for any proper ideal $\mathfrak{c}$ by Lemma 8, this may be established by showing that $\mathscr{E}(\mathfrak{a}:(\gamma)) \subseteqq \mathscr{E}(\mathfrak{a})$. Above, this inclusion appears as a consequence of

Lemma 6; however, it might also be obtained without the intervention of the concept of $\mathfrak{a}$-extremal multiplicatively closed sets, based on the equation $F(\mathfrak{a}(\mathfrak{p})) = \complement\mathfrak{p}$ for the definition of $\mathscr{E}(\mathfrak{a})$, as follows: If $\mathfrak{p} \in \mathscr{E}(\mathfrak{a}:(\gamma))$, i.e., $F(\mathfrak{a}:(\gamma)\,(\mathfrak{p})) = \complement\mathfrak{p}$ then, by Lemma 2, $\mathfrak{a}:(\gamma)\,(\mathfrak{p}) = \mathfrak{a}(\mathfrak{p}):(\gamma)$. Next, one proves $F(\mathfrak{c}) \subseteqq F(\mathfrak{c}:(\gamma))$ for any ideal $\mathfrak{c}$ and any $\gamma \in \mathfrak{o}$ and thus obtains $F(\mathfrak{a}(\mathfrak{p})) \subseteqq F(\mathfrak{a}(\mathfrak{p}):(\gamma)) = \complement\mathfrak{p}$ from which $F(\mathfrak{a}(\mathfrak{p})) = \complement\mathfrak{p}$ finally follows. Similarly, a proof for Lemma 6 may be given which uses the equation $F(\mathfrak{a}_S) = S$ to establish $\mathfrak{a}$-extremality.

A further consequence of Proposition 1 is the following improvement of another result of [2]:

Corollary. *For any ideal* $\mathfrak{a}$, $F(\mathfrak{a}) = \complement \bigcup \mathfrak{p}\ (\mathfrak{p} \in \mathscr{E}(\mathfrak{a}))$.

Proof. $F(\mathfrak{a}) \subseteqq \complement\mathfrak{p}$ for each $\mathfrak{p} \in \mathscr{E}(\mathfrak{a})$ by the corollary 1 of Lemma 3, hence $S = \bigcap \complement\mathfrak{p}\,(\mathfrak{p} \in \mathscr{E}(\mathfrak{a}))$ contains $F(\mathfrak{a})$. On the other hand, $\mathfrak{a}_S \subseteqq \mathfrak{a}(\mathfrak{p})$ for each $\mathfrak{p} \in \mathscr{E}(\mathfrak{a})$ and hence, by Proposition 1, $\mathfrak{a}_S \subseteqq \mathfrak{a}$; this implies $S \subseteqq F(\mathfrak{a})$.

This corollary is a special instance of the following general observation: If S_α, $\alpha \in I$, is a family of $\mathfrak{a}$-extremal multiplicatively closed sets such that $\mathfrak{a} = \bigcap \mathfrak{a}_{S_\alpha} (\alpha \in I)$ then $F(\mathfrak{a}) = \bigcap S_\alpha\ (\alpha \in I)$.

3. The component theorems. With the results obtained so far it is now possible to give simple proofs for desired generalizations to arbitrary ideals of the three statements considered in the introduction. The first of these is an immediate consequence of Lemma 4 and does not, in particular, depend on Proposition 1[2]).

Proposition 2. *For any component* $\mathfrak{a}_S$ *of* $\mathfrak{a}$, $\mathscr{E}(\mathfrak{a}_S) = \{\mathfrak{p} \mid \mathfrak{p} \in \mathscr{E}(\mathfrak{a})$ *and* $\mathfrak{p} \cap S = \varnothing\}$.

Proof. If $\mathfrak{a}_S = \mathfrak{o}$ then $\mathscr{E}(\mathfrak{a}_S) = \varnothing$ whilst $\mathfrak{p} \cap S = \varnothing$, $\mathfrak{p} \in \mathscr{E}(\mathfrak{a})$, would imply that $\mathfrak{o} = \mathfrak{a}_S \subseteqq \mathfrak{a}(\mathfrak{p}) \subseteqq \mathfrak{p} \subset \mathfrak{o}$, a contradiction which shows $\{\mathfrak{p} \mid \mathfrak{p} \in \mathscr{E}(\mathfrak{a}), \mathfrak{p} \cap S = \varnothing\}$ is also void. It remains to consider the case $\mathfrak{a}_S \neq \mathfrak{o}$; here, one has $\mathscr{E}(\mathfrak{a}_S) \neq \varnothing$. If $\mathfrak{p} \in \mathscr{E}(\mathfrak{a}_S)$ then $\mathfrak{p} \supseteqq \mathfrak{a}_S$ and $\complement\mathfrak{p}$ is $\mathfrak{a}_S$-extremal. Hence, $\mathfrak{p} \supseteqq \mathfrak{a}$, $\complement\mathfrak{p} \supseteqq S$ and $\complement\mathfrak{p}$ is $\mathfrak{a}$-extremal, i.e., $\mathfrak{p} \in \mathscr{E}(\mathfrak{a})$ and $\mathfrak{p} \cap S = \varnothing$. Conversely, if this holds for $\mathfrak{p}$ then $S \subseteqq \complement\mathfrak{p}$, hence $\complement\mathfrak{p}$ is $\mathfrak{a}_S$-extremal, and $\mathfrak{p} \supseteqq \mathfrak{a}_S$ since $\mathfrak{p} \supseteqq \mathfrak{a}(\mathfrak{p}) \supseteqq \mathfrak{a}_S$; thus $\mathfrak{p} \in \mathscr{E}(\mathfrak{a}_S)$.

This proposition and Proposition 1 together now lead to

Proposition 3. *For any* S, T, *if* $\mathfrak{p} \cap S = \varnothing$ *iff* $\mathfrak{p} \cap T = \varnothing$ $(\mathfrak{p} \in \mathscr{E}(\mathfrak{a}))$ *then* $\mathfrak{a}_S = \mathfrak{a}_T$.

Proof. Here, $\mathscr{E}(\mathfrak{a}_S) = \mathscr{E}(\mathfrak{a}_T)$ and for any $\mathfrak{p}$ in this set one has $\mathfrak{a}_S(\mathfrak{p}) = \mathfrak{a}(\mathfrak{p}) = \mathfrak{a}_T(\mathfrak{p})$ since $\mathfrak{p} \supseteqq S, T$. Hence $\mathfrak{a}_S = \bigcap \mathfrak{a}(\mathfrak{p})\ (\mathfrak{p} \in \mathscr{E}(\mathfrak{a}_S)) = \mathfrak{a}_T$.

Finally, a characterization of the sets $\mathscr{E}(\mathfrak{a}_S) \subseteqq \mathscr{E}(\mathfrak{a})$ is to be given which is independent of the notion of component ideal. This will be done by means of the following concept:

Definition. *A set* $\mathscr{X} \subseteqq \mathscr{E}(\mathfrak{a})$ *is closed in* $\mathscr{E}(\mathfrak{a})$ *iff* $\mathfrak{r} \subseteqq \bigcup \mathfrak{p}\,(\mathfrak{p} \in \mathscr{X})$, $\mathfrak{r} \in \mathscr{E}(\mathfrak{a})$, *implies* $\mathfrak{r} \in \mathscr{X}$.

Now one has:

Proposition 4. *For any component* $\mathfrak{a}_S$ *of* $\mathfrak{a}$, $\mathscr{E}(\mathfrak{a}_S)$ *is closed in* $\mathscr{E}(\mathfrak{a})$ *and for any* $\mathscr{X} \subseteqq \mathscr{E}(\mathfrak{a})$ *closed in* $\mathscr{E}(\mathfrak{a})$ *there exists an* S *such that* $\mathscr{E}(\mathfrak{a}_S) = \mathscr{X}$.

Proof. Since $\mathscr{E}(\mathfrak{a}_S) = \{\mathfrak{p} \mid \mathfrak{p} \in \mathscr{E}(\mathfrak{a})$ and $\mathfrak{p} \cap S = \varnothing\}$ one has that $\bigcup \mathfrak{p}\ (\mathfrak{p} \in \mathscr{E}(\mathfrak{a}_S)) \subseteqq \complement S$, hence $\mathfrak{r} \subseteqq \bigcup \mathfrak{p}\ (\mathfrak{p} \in \mathscr{E}(\mathfrak{a}_S))\ (\mathfrak{r} \in \mathscr{E}(\mathfrak{a}))$ implies $\mathfrak{r} \cap S = \varnothing$ and thus $\mathfrak{r} \in \mathscr{E}(\mathfrak{a}_S)$. Conversely, let $\mathscr{X}$ be closed in $\mathscr{E}(\mathfrak{a})$ and put $S = \complement \bigcup \mathfrak{p}\,(\mathfrak{p} \in \mathscr{X})$. Then, $\mathscr{E}(\mathfrak{a}_S) = \{\mathfrak{p} \mid \mathfrak{p} \in \mathscr{E}(\mathfrak{a})$ and $\mathfrak{p} \cap S = \varnothing\} \supseteqq \mathscr{X}$ and $\mathfrak{r} \in \mathscr{E}(\mathfrak{a}_S)$ implies that $\mathfrak{r} \subseteqq \complement S = \bigcup \mathfrak{p}\,(\mathfrak{p} \in \mathscr{X})$, hence that $\mathfrak{r} \in \mathscr{X}$. Therefore, one has $\mathscr{E}(\mathfrak{a}_S) = \mathscr{X}$.

---

[2]) J.-M. MARANDA informs me that he also has proofs for the next two propositions.

Remark. For a finite $\mathscr{E}(\mathfrak{a})$, the closed $\mathscr{X}$ in $\mathscr{E}(\mathfrak{a})$ are exactly the isolated subsets of $\mathscr{E}(\mathfrak{a})$ since, for finite $\mathscr{X}$, $\mathfrak{r} \subseteqq \bigcup \mathfrak{p}\,(\mathfrak{p} \in \mathscr{X})$ holds iff $\mathfrak{r} \subseteqq \mathfrak{p}$ for some $\mathfrak{p} \in \mathscr{X}$ [3]. This shows that for decomposable $\mathfrak{a}$ Proposition 4 reduces to the theorem about components of which the statement III in the introduction is one part.

A somewhat more complete, and perhaps more expressive description of the relation between the set $\mathscr{C}(\mathfrak{a})$ of all components $\mathfrak{c}$ of $\mathfrak{a}$ and the set $\Omega(\mathfrak{a})$ of all $\mathscr{X} \subseteqq \mathscr{E}(\mathfrak{a})$ closed in $\mathscr{E}(\mathfrak{a})$ may be given as follows: *There is a one-to-one order inverting correspondence between* $\mathscr{C}(\mathfrak{a})$ *and* $\Omega(\mathfrak{a})$ *given by* $\mathfrak{c} \to \mathscr{E}(\mathfrak{c}) = \{\mathfrak{p} \mid \mathfrak{p} \in \mathscr{E}(\mathfrak{a})$ *and* $\mathfrak{p} \cap F(\mathfrak{c}) = \varnothing\}$ *and its inverse* $\mathscr{X} \to \mathfrak{a}(\mathscr{X}) = \bigcap \mathfrak{a}(\mathfrak{p})\,(\mathfrak{p} \in \mathscr{X})$. To see this one merely has to observe that $\mathfrak{c} = \bigcap \mathfrak{a}(\mathfrak{p})\,(\mathfrak{p} \in \mathscr{E}(\mathfrak{c}))$, $\mathscr{E}(\mathfrak{a}(\mathscr{X})) = \mathscr{X}$ and that for components $\mathfrak{c}_1, \mathfrak{c}_2$ of $\mathfrak{a}$ $\mathfrak{c}_1 \subseteqq \mathfrak{c}_2$ implies $F(\mathfrak{c}_1) \subseteqq F(\mathfrak{c}_2)$.

Another comment that can be made on the basis of Proposition 4 concerns the closure system $\mathscr{S}(\mathfrak{a})$ of all $\mathfrak{a}$-extremal multiplicatively closed sets in the closure system $\mathscr{S}$ of all multiplicatively closed sets, namely: $\mathscr{S}(\mathfrak{a})$ *is generated by its subset* $\{\complement\mathfrak{p} \mid \mathfrak{p} \in \mathscr{E}(\mathfrak{a})\}$ *and hence the closure operator on* $\mathscr{S}$ *associated with* $\mathscr{S}(\mathfrak{a})$ *is* $S \to \bigcap \complement\mathfrak{p}\,(\mathfrak{p} \in \mathscr{E}(\mathfrak{a}),\ S \subseteqq \complement\mathfrak{p})$. This follows from the equations $S = F(\mathfrak{a}_S) = \bigcap \complement\mathfrak{p}\,(\mathfrak{p} \in \mathscr{E}(\mathfrak{a}),\ S \cap \mathfrak{p} = \varnothing)$ for $S \in \mathscr{S}(\mathfrak{a})$. Furthermore, the relation between $\mathscr{C}(\mathfrak{a})$ and $\Omega(\mathfrak{a})$ induces the following relation between $\mathscr{S}(\mathfrak{a})$ and $\Omega(\mathfrak{a})$: *There is a one-to-one order inverting correspondence between* $\mathscr{S}(\mathfrak{a})$ *and* $\Omega(\mathfrak{a})$ *given by* $S \to \mathscr{X}(S) = \{\mathfrak{p} \mid \mathfrak{p} \in \mathscr{E}(\mathfrak{a}), S \cap \mathfrak{p} = \varnothing\}$ *and its inverse* $\mathscr{X} \to S(\mathscr{X}) = \bigcap \complement\mathfrak{p}\,(\mathfrak{p} \in \mathscr{X})$. This is a consequence of the fact that $S \to \mathfrak{a}_S$ and $\mathfrak{c} \to F(\mathfrak{c})$ are one-to-one order preserving mappings, inverse to each other, of $\mathscr{S}(\mathfrak{a})$ onto $\mathscr{C}(\mathfrak{a})$ and $\mathscr{C}(\mathfrak{a})$ onto $\mathscr{S}(\mathfrak{a})$ respectively, and that $\mathscr{X}(S) = \mathscr{E}(\mathfrak{a}_S)$ and $S(\mathscr{X}) = F(\mathfrak{a}(\mathscr{X}))$.

4. Rings without unit. So far, the ring $\mathfrak{o}$ under consideration was assumed to possess a unit. It will now be shown that the results obtained above also hold if $\mathfrak{o}$ is taken to be a ring without unit. To this end, a number of new conventions are necessary which take into account the absence of the unit. These are:

(i) $\mathfrak{o}$ itself is also considered as a prime ideal.
(ii) the void set $\varnothing$ is also considered as a multiplicatively closed set.
(iii) $\mathfrak{a}_\varnothing = \mathfrak{a}$ for each ideal $\mathfrak{a}$.
(iv) $S\varnothing = \varnothing S = S$ for any S.

In a sense, this makes $\varnothing$ play a rôle similar to that of the multiplicatively closed set $\{1\}$ in a ring with unit 1. With these conventions, Lemmas 1 and 2 are easily seen to still hold for $\mathfrak{o}$.

The definition of $\mathfrak{a}$-extremal multiplicatively closed sets remains the same as before. In particular, this means that $\varnothing$ is $\mathfrak{a}$-extremal iff $\mathfrak{a} \subset \mathfrak{a}_S$ for any $S \neq \varnothing$. Concerning the validity of Lemma 3 in the present situation one observes that for $S \neq \varnothing$ the same proof works whilst for $S = \varnothing$ the lemma states that $\varnothing$ is $\mathfrak{a}$-extremal iff $\mathfrak{a}_T = \mathfrak{a}$ implies $T = \varnothing$ which is obviously so. The corollaries of Lemma 3 follow now as before. As to Lemma 4, nothing has to be proved if $S = \varnothing$; for $T = \varnothing$ it states that $\varnothing$ is $\mathfrak{a}_S$-extremal iff $S = \varnothing$ and $\varnothing$ is $\mathfrak{a}$-extremal, which again follows readily from the definition of $\mathfrak{a}$-extremality. The remaining lemmas of the first section, being formal consequences of the first four, are hereby also established to hold. In particular, one has that $\varnothing$ is $\mathfrak{a}$-extremal iff $F(\mathfrak{a}) = \varnothing$.

The $\mathfrak{a}$-extremal prime ideals are, of course, defined in the same way as before. Regarding the further lemmas one finds that Lemma 7, being a consequence of Lemma 5, clearly holds; Lemma 8, however, requires some consideration of the case that $\mathfrak{o}$ is a prime ideal minimal above $\mathfrak{a}$. Here, assume $\mathfrak{a} \cap F(\mathfrak{a}) = \varnothing$ and $F(\mathfrak{a}) \neq \varnothing$. Then, for any $\mathfrak{r} \supseteqq \mathfrak{a}$ maximal such that $\mathfrak{r} \cap F(\mathfrak{a}) = \varnothing$ one has $\mathfrak{a} \subseteqq \mathfrak{r} \subset \mathfrak{o}$, a contradiction since $\mathfrak{r}$ is prime; hence it follows that either $F(\mathfrak{a}) = \varnothing$ or $\mathfrak{a} \cap F(\mathfrak{a}) \neq \varnothing$. The former of these conditions implies $\mathfrak{o} \in \mathscr{E}(\mathfrak{a})$ whereas the latter gives $\mathfrak{a} = \mathfrak{o}$. Since $\mathfrak{o}$ is not $\mathfrak{o}$-extremal ($\varnothing = \complement\mathfrak{o}$ not being such) this shows that $\mathfrak{a} = \mathfrak{o}$ must be excluded. Hence one has now that Lemma 8 holds for any proper $\mathfrak{a}$. Finally, Lemma 9 can be proved in the present situation. The case $\mathfrak{a}:(\gamma) \subset \mathfrak{o}$ is covered by the same proof as before. On the other hand, $\mathfrak{a}:(\gamma) = \mathfrak{o}$, i.e., $\gamma\mathfrak{o} \subseteqq \mathfrak{a}$, implies $\gamma \in \mathfrak{a}_S$ for any $S \supset \varnothing$ and since $\gamma \notin \mathfrak{a}$ this shows that $\mathfrak{a}_S \supset \mathfrak{a}$; thus $\varnothing$ is $\mathfrak{a}$-extremal, i.e., $\mathfrak{o} \in \mathscr{E}(\mathfrak{a})$, and $\gamma \notin \mathfrak{a} = \mathfrak{a}_\varnothing = \mathfrak{a}(\mathfrak{o})$.

On the basis of these observations it follows that the proofs of Propositions 1 to 4 and the Corollary of Proposition 1 are still valid in the present situation and it is thus seen that these results also hold for rings without unit.

5. Decomposable ideals. It may be of interest to give a proof of the First Uniqueness Theorem for primary decompositions of decomposable ideals [4] based on the results and techniques of the preceeding sections.

First, the following characterization, given in [2], of the primary ideals is required here:

Lemma 10. *If* $\mathfrak{q}$ *is primary (proper if the ring has no unit) then* $\mathscr{E}(\mathfrak{q}) = \{\sqrt{\mathfrak{q}}\}$ *and if* $\mathscr{E}(\mathfrak{a}) = \{\mathfrak{p}\}$ *then* $\mathfrak{a}$ *is primary.*

Proof. For a primary ideal $\mathfrak{q}$, $\sqrt{\mathfrak{q}}$ is a minimal prime ideal (in fact, the only one) above $\mathfrak{q}$ and hence $\sqrt{\mathfrak{q}} \in \mathscr{E}(\mathfrak{q})$. Now, it follows from the definition of primary ideals that $F(\mathfrak{q}) = \mathbf{C}\sqrt{\mathfrak{q}}$. Hence, for any $\mathfrak{q} \in \mathscr{E}(\mathfrak{q})$, $\mathbf{C}\mathfrak{p} \supseteq \mathbf{C}\sqrt{\mathfrak{q}}$, i.e., $\mathfrak{p} \subseteqq \sqrt{\mathfrak{q}}$ and thus $\mathfrak{p} = \sqrt{\mathfrak{q}}$. Conversely, if $\mathscr{E}(\mathfrak{a}) = \{\mathfrak{p}\}$ then $\mathfrak{p}$ is a minimal prime ideal above $\mathfrak{a}$ and $\mathfrak{a} = \mathfrak{a}(\mathfrak{p})$ by Proposition 1. Since it is known that, for any $\mathfrak{a}$ and prime ideal $\mathfrak{p}$ minimal above $\mathfrak{a}$, $\mathfrak{a}(\mathfrak{p})$ is primary, this completes the proof.

Next, a relation is obtained for certain $\mathscr{E}(\mathfrak{a})$ which plays a role in the proof of the First Uniqueness Theorem.

Lemma 11. *If* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *are ideals such that each* $\mathscr{E}(\mathfrak{a}_i)$ *is finite then* $\mathscr{E}(\mathfrak{a}) \subseteqq \bigcup \mathscr{E}(\mathfrak{a}_i)$ *for* $\mathfrak{a} = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$.

Proof. For $\mathfrak{p} \in \mathscr{E}(\mathfrak{a})$ one has $\mathfrak{a}(\mathfrak{p}) = \mathfrak{a}_1(\mathfrak{p}) \cap \ldots \cap \mathfrak{a}_n(\mathfrak{p})$. Now, put $S_i = F(\mathfrak{a}_i(\mathfrak{p})) = \bigcap \mathbf{C}\mathfrak{r}\,(\mathfrak{p} \supseteqq \mathfrak{r} \in \mathscr{E}(\mathfrak{a}_i))$ and $S = S_1 \cap \ldots \cap S_n$. Then, $\mathfrak{a}_S = (\mathfrak{a}_1)_S \cap \ldots \cap (\mathfrak{a}_n)_S \subseteqq (\mathfrak{a}_1)_{S_1} \cap \ldots \cap (\mathfrak{a}_n)_{S_n} = \mathfrak{a}(\mathfrak{p})$, and it follows from $\mathfrak{p} \in \mathscr{E}(\mathfrak{a})$ that $S \subseteqq \mathbf{C}\mathfrak{p}$; on the other hand, $\mathbf{C}\mathfrak{p} \subseteqq S_i$ for each i and hence $S = \mathbf{C}\mathfrak{p}$. Thus, one has $\mathfrak{p} = \bigcup \mathbf{C}S_i = \bigcup \mathfrak{r}\,(\mathfrak{p} \supseteqq \mathfrak{r} \in \mathscr{E}(\mathfrak{a}_i);\ i = 1, \ldots, n)$. Since each $\mathscr{E}(\mathfrak{a}_i)$ is finite it follows [3] that $\mathfrak{p} = \mathfrak{r}$ for some $\mathfrak{r}$ in some $\mathscr{E}(\mathfrak{a}_i)$.

An immediate consequence of the two preceeding lemmas is the following well-known result:

Corollary. *If* $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ *are primary ideals with the same radical* $\mathfrak{p}$ *then* $\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ *is also primary with radical* $\mathfrak{p}$.

Proof. One has $\mathscr{E}(\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n) \subseteqq \bigcup \mathscr{E}(\mathfrak{q}_i) = \{\mathfrak{p}\}$ and hence $\mathscr{E}(\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n) = \{\mathfrak{p}\}$, unless, in the case of a ring without unit, all $\mathfrak{q}_i$ are the whole ring $\mathfrak{o}$, and then the statement is trivial.

The final lemma to be used here is

Lemma 12. *If* $\mathfrak{q}$ *is primary and* $\mathfrak{a} \nsubseteqq \mathfrak{q}$ *then* $\sqrt{\mathfrak{q}} \in \mathscr{E}(\mathfrak{a} \cap \mathfrak{q})$.

Proof. Let $\mathfrak{c} = \mathfrak{a} \cap \mathfrak{q}$; then, for any $S \supset \mathbf{C}\sqrt{\mathfrak{q}}$, $\mathfrak{c}_S = \mathfrak{a}_S$. Now, suppose $\mathfrak{c}_S = \mathfrak{c}(\sqrt{\mathfrak{q}})$. This implies $\mathfrak{c}_S = \mathfrak{a}(\sqrt{\mathfrak{q}}) \cap \mathfrak{q}$ and hence $\mathfrak{c} = \mathfrak{a} \cap \mathfrak{q} = \mathfrak{c}_S \cap \mathfrak{a} = \mathfrak{a}_S \cap \mathfrak{a} = \mathfrak{a}$ or $\mathfrak{a} \subseteqq \mathfrak{q}$, a contradiction. It follows that $\mathfrak{c}_S \supset \mathfrak{c}(\sqrt{\mathfrak{q}})$ which shows that $\sqrt{\mathfrak{q}} \in \mathscr{E}(\mathfrak{c})$.

These lemmas now lead to a very simple proof of the following result, due to Krull [2], on normal decompositions of decomposable ideals $\mathfrak{a}$, i.e., intersection representations $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$, $\mathfrak{q}_i$ primary, for which (i) the $\sqrt{\mathfrak{q}_i}$ are distinct and (ii) $\bigcap \mathfrak{q}_j \nsubseteqq \mathfrak{q}_i$ $(j \neq i)$ for each i.

Proposition 5. *If* $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ *(normal) then* $\mathscr{E}(\mathfrak{a}) = \{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\}$.

Proof. One has $\mathscr{E}(\mathfrak{a}) \subseteqq \{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\}$ by Lemma 10 and 11 and $\{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\} \subseteqq \mathscr{E}(\mathfrak{a})$ by Lemma 12.

Obviously, this proposition implies immediately that for all normal decompositions of a decomposable ideal the numbers of the occurring primary ideals and, moreover, the sets of radicals of these are the same, i. e., the First Uniqueness Theorem.

References

[1] B. Banaschewski, Zur Idealtheorie der ganzen Funktionen. Math. Nachr. **19**, 136—160 (1958).
[2] W. Krull, Idealtheorie in Ringen ohne Endlichkeitsbedingungen. Math. Ann. **101**, 729—744 (1929).
[3] D. G. Northcott, Ideal Theory. Cambridge University Press 1953.
[4] B. L. van der Waerden, Moderne Algebra II. Julius Springer, Berlin 1940.

Eingegangen am 19. 9. 1960

Anschrift des Autors:

Bernhard Banaschewski
Department of Mathematics
Hamilton College
McMaster University
Hamilton (Ontario), Canada

Zum Primbasissatz in regulären lokalen Ringen

Von

HANS-JOACHIM NASTOLD

Alle im folgenden auftretenden Ringe seien noethersch, kommutativ und mit 1-Element. Das Ziel dieser Note ist eine Verschärfung des Primbasissatzes für reguläre lokale Ringe. Der Begriff der *Primbasis* wurde für Polynomringe von W. GRÖBNER (s. z. B. [2]) geprägt. Während es Primideale $\mathfrak{p}$ vom Rang $r(\mathfrak{p}) = s$ mit beliebig großer minimaler Erzeugendenanzahl gibt (vgl. [2], S. 115, Fußnote), *liefert eine Primbasis für jedes Primideal $\mathfrak{p}$ vom Rang s eine Darstellung, die mit $s+1$ Elementen auskommt,* und zwar eine Darstellung der Form $\mathfrak{p} = (a_1, \ldots, a_s):t$.

$\mathfrak{p}$ besteht also gerade aus der Menge aller Elemente x mit der Eigenschaft

$$tx \in (a_1, \ldots, a_s).$$

In dieser schwächsten Form gilt der *Primbasissatz für beliebige noethersche Ringe A* (s. [3], chap. III, Theorem 1, Cor. 4): Man hat für $a_1, \ldots, a_s$ lediglich ein System von s Elementen aus $\mathfrak{p}$ zu nehmen, die in dem nach $\mathfrak{p}$ lokalisierten Ring $A_{\mathfrak{p}}$ ein Definitionsideal (ein zum maximalen Ideal $\mathfrak{p}A_{\mathfrak{p}}$ primäres Ideal) erzeugen. Nach einer kennzeichnenden Eigenschaft der Dimension gibt es nämlich sicher in $A_{\mathfrak{p}}$ s solche Elemente $a'_1, \ldots, a'_s$. Multiplikation mit deren Hauptnenner, einer Einheit in $A_{\mathfrak{p}}$, liefert dann das gewünschte Elementsystem $a_1, \ldots, a_s \in A$. $\mathfrak{p}$ ist somit minimales Primoberideal von $(a_1, \ldots, a_s)$, also assoziiert zu $A/(a_1, \ldots, a_s)$. Nach SERRE [3], chap. I, ist $\mathfrak{p}$ dann Annullator eines Elementes $\bar{t}$ von $A/(a_1, \ldots, a_s)$:

$$\mathfrak{p} = 0:(\bar{t}) = 0:\bar{t} \text{ in } A/(a_1, \ldots, a_s).$$

Für ein Element $t \in \bar{t}$ aus A gilt dann $\mathfrak{p} = (a_1, \ldots, a_s):t$ in A.

Für manche Zwecke ist es nützlich, eine Primbasisdarstellung $\mathfrak{p} = (a_1, \ldots, a_s):t$ mit der Eigenschaft $t \notin \mathfrak{p}$ zur Verfügung zu haben. Eine solche ist nicht mehr für jedes Primideal $\mathfrak{p}$ möglich. Es gilt:

Genau dann existiert für das Primideal $\mathfrak{p}$ vom Rang $r(\mathfrak{p}) = s$ eine Primbasisdarstellung $\mathfrak{p} = (a_1, \ldots, a_s):t$ mit $t \notin \mathfrak{p}$, wenn $A_{\mathfrak{p}}$ regulär ist. Man hat hierzu für $a_1, \ldots, a_s$ ein System von s Elementen aus $\mathfrak{p}$ zu wählen, die im lokalisierten Ring $A_{\mathfrak{p}}$ das maximale Ideal $\mathfrak{p}A_{\mathfrak{p}}$ erzeugen: $\mathfrak{p}A_{\mathfrak{p}} = (a_1, \ldots, a_s)_{\mathfrak{p}}$.

Beweis. $\mathfrak{p} = (a_1, \ldots, a_s):t$, $t \notin \mathfrak{p}$, hat $\mathfrak{p}A_{\mathfrak{p}} = (a_1, \ldots, a_s)_{\mathfrak{p}}$ zur Folge. Das maximale Ideal $\mathfrak{p}A_{\mathfrak{p}}$ des lokalen Ringes $A_{\mathfrak{p}}$ der Dimension $s = r(\mathfrak{p})$ läßt sich somit durch s Elemente erzeugen. Ist umgekehrt $A_{\mathfrak{p}}$ regulär, so gibt es s Elemente $a'_1, \ldots, a'_s$ mit $\mathfrak{p}A_{\mathfrak{p}} = (a'_1, \ldots, a'_s)_{\mathfrak{p}}$. Multiplikation mit dem Hauptnenner der a'_k, einer Einheit in

$A_{\mathfrak{p}}$, liefert ein System $a_1, \ldots, a_s$ mit $\mathfrak{p} A_{\mathfrak{p}} = (a_1, \ldots, a_s)_{\mathfrak{p}}$. Ist nun $\mathfrak{p} = (p_1, \ldots, p_r)$, so besitzt jedes p_i eine Darstellung

$$p_i = \sum_{k=1}^{s} b_{ik} a_k, \quad b_{ik} \in A_{\mathfrak{p}}.$$

Mit $t_i \notin \mathfrak{p}$ als Hauptnenner der b_{ik}, $k = 1, \ldots, s$, ist also $t_i p_i \in (a_1, \ldots, a_s)$. Für $t = \prod_i t_i \notin \mathfrak{p}$ gilt dann $t p_i \in (a_1, \ldots, a_s)$, $i = 1, \ldots, r$, d. h. es ist $t\mathfrak{p} \subset (a_1, \ldots, a_s)$. Wegen $t \notin \mathfrak{p}$, $(a_1, \ldots, a_s) \subset \mathfrak{p}$ folgt aber aus $tx \in (a_1, \ldots, a_s)$ $x \in \mathfrak{p}$, d. h. es ist tatsächlich $\mathfrak{p} = (a_1, \ldots, a_s) : t$ mit $t \notin \mathfrak{p}$. Offenbar gibt es für $r(\mathfrak{p}) = s$ keine solche Darstellung mit weniger als s Elementen a_k.

Eine Folge von Elementen $a_1, \ldots, a_s$ aus dem Jacobson *Radikal* $\mathfrak{r}(A)$, dem Durchschnitt aller maximalen Ideale von A, heißt eine *A-Folge*, wenn die Sequenzen

$$0 \to A_{i-1} \xrightarrow{a_i} A_{i-1} \to A_i \to 0, \quad i = 1, \ldots, s, A_0 = A, A_i = A/(a_1, \ldots, a_i)$$

exakt sind. Der zweite Pfeil bedeutet dabei die durch Multiplikation mit a_i entstehende Abbildung. a_1 ist also Nichtnullteiler von A, a_2 Nichtnullteiler von $A_1 = A/(a_1), \ldots, a_i$ Nichtnullteiler von $A_{i-1} = A/(a_1, \ldots, a_{i-1})$. Ein semilokaler Ring A, d. i. ein Ring mit nur endlich vielen maximalen Idealen, heißt ein *Cohen-Macaulay-Ring*, wenn er von der (Krullschen) Dimension $\dim A = n$ ist und eine A-Folge derselben Länge n besitzt.

Wir beweisen nun den folgenden

Satz 1. *Ist A ein semilokaler Cohen-Macaulay-Ring, $\mathfrak{p} \subset \mathfrak{r}(A)$ ein Primideal des Ranges $r(\mathfrak{p}) = s$ und $A_{\mathfrak{p}}$ regulär, so gibt es s Elemente $a_1, \ldots, a_s \in \mathfrak{p}$ mit $(a_1, \ldots, a_s)_{\mathfrak{p}} = \mathfrak{p} A_{\mathfrak{p}}$ und $r(a_1, \ldots, a_s) = s$.*

Die s Elemente bilden dann eine A-Folge, denn sie erzeugen ein Ideal $(a_1, \ldots, a_s) \subset \mathfrak{p}$ vom Rang s.

In der letzteren Eigenschaft des Elementsystems $a_1, \ldots, a_s$ besteht unsere Verschärfung des Primbasissatzes.

Beweis. Durch Induktion nach s mit

Hilfssatz 1. *Ist A ein äquidimensionaler Ring (d. h. alle zum 0-Ideal assoziierten Primideale von A sind vom Rang 0; dies ist sicher der Fall, wenn A Cohen-Macaulay-Ring ist* [1], [3], *chap.* IV*) und $\mathfrak{a} \subset A$ ein Ideal des Ranges $r(\mathfrak{a}) = s \geqq 1$, so besitzt $\mathfrak{a}$ ein Erzeugendensystem aus lauter Nichtnullteilern.*

Beweis. Es seien $y_1, \ldots, y_r$ ein Erzeugendensystem des Ideals $\mathfrak{a}$ und $\mathfrak{n}_1, \ldots, \mathfrak{n}_n$ die zum 0-Ideal in A assoziierten Primideale, also nach Voraussetzung $r(\mathfrak{n}_\nu) = 0$, $\nu = 1, \ldots, n$. Die Nullteiler von A sind dann gerade die Elemente aus $\bigcup_{\nu=1}^{n} \mathfrak{n}_\nu$. Nun ist sicher ein y_i, etwa y_1, nicht enthalten in der Vereinigung $\bigcup_{\nu=1}^{n} \mathfrak{n}_\nu$. Denn wären alle $y_i \in \bigcup_{\nu=1}^{n} \mathfrak{n}_\nu$, so wäre $\mathfrak{a} \subset \bigcup_{\nu=1}^{n} \mathfrak{n}_\nu$, also nach einem bekannten Satz (vgl. z. B. SERRE [3], chap. I, S. 3) $\mathfrak{a} \subset \mathfrak{n}_{\nu_0}$ für ein geeignetes ν_0. Dann wäre jedoch $r(\mathfrak{a}) = 0$, entgegen

$r(\mathfrak{a}) = s \geqq 1$. Wir ersetzen nun die übrigen y_k, $k = 2, \ldots, r$, durch Elemente $y'_k = z_k y_1 + y_k$ mit geeignet gewählten $z_k \in A$, so daß $y'_k \notin \bigcup_{\nu=1}^{n} \mathfrak{n}_\nu$. Das so entstandene System $y'_1 = y_1, y'_2, \ldots, y'_r$ ist dann offenbar wieder ein Erzeugendensystem von $\mathfrak{a}$ und die y'_i sind nun alle Nichtnullteiler. Ist $y_k \in \mathfrak{n}_1, \ldots, \mathfrak{n}_n$, so setzen wir $z_k = 1$; ist $y_k \in \mathfrak{n}_1, \ldots, \mathfrak{n}_m$, $y_k \notin \mathfrak{n}_{m+1}, \ldots, \mathfrak{n}_n$, so wählen wir z_k so, daß $z_k \notin \mathfrak{n}_1, \ldots, \mathfrak{n}_m$, $z_k \in \mathfrak{n}_{m+1}, \ldots, \mathfrak{n}_n$. Ein solches z_k gibt es sicher: Anderenfalls wäre $\mathfrak{n}_{m+1} \cap \ldots \cap \mathfrak{n}_n \subset \mathfrak{n}_1 \cup \cdots \cup \mathfrak{n}_m$. Dann wäre aber für ein μ_0 mit $1 \leqq \mu_0 \leqq m$ $\mathfrak{n}_{m+1} \cap \cdots \cap \mathfrak{n}_n \subset \mathfrak{n}_{\mu_0}$, also für ein ν_0 mit $m + 1 \leqq \nu_0 \leqq n$ $\mathfrak{n}_{\nu_0} \subset \mathfrak{n}_{\mu_0}$, was nicht sein kann. Nach Wahl von z_k ist nun $z_k y_1 \notin \mathfrak{n}_1, \ldots, \mathfrak{n}_m$, aber $\in \mathfrak{n}_{m+1}, \ldots, \mathfrak{n}_n$, also $y'_k = z_k y_1 + y_k \notin \bigcup_{\nu=1}^{n} \mathfrak{n}_\nu$, was zu zeigen war.

Aus Hilfssatz 1 ergibt sich

Hilfssatz 2. *Ist A ein äquidimensionaler Ring, $\mathfrak{p} \subset A$ ein Primideal des Ranges $r(\mathfrak{p}) = s \geqq 1$ und $A_\mathfrak{p}$ regulär, so gibt es s Nichtnullteiler $x_1, \ldots, x_s \in \mathfrak{p}$ mit $(x_1, \ldots, x_s)_\mathfrak{p} = \mathfrak{p} A_\mathfrak{p}$.*

Beweis. Nach Hilfssatz 1 gibt es ein Erzeugendensystem $y_1, \ldots, y_r$ von $\mathfrak{p}$ aus lauter Nichtnullteilern, so daß $(y_1, \ldots, y_r)_\mathfrak{p} = \mathfrak{p} A_\mathfrak{p}$. Aus dem Erzeugendensystem $y_1, \ldots, y_r$ von $\mathfrak{p} A_\mathfrak{p}$ lassen sich s Elemente $x_1, \ldots, x_s$ auswählen, die $\mathfrak{p} A_\mathfrak{p}$ schon erzeugen: $(x_1, \ldots, x_s)_\mathfrak{p} = \mathfrak{p} A_\mathfrak{p}$.

Nun zum Beweis von Satz 1: Für $s = 0$ ist $A_\mathfrak{p}$ ein Körper, also $\mathfrak{p} A_\mathfrak{p} = (0)$ und unsere Behauptung wird durch die aus 0 Elementen bestehende leere Menge erfüllt. Es sei daher $s \geqq 1$ und unsere Behauptung für Primideale des Ranges $s - 1$ schon bewiesen. Für ein Primideal $\mathfrak{p} \subset \mathfrak{r}(A)$ mit $r(\mathfrak{p}) = s$ und $A_\mathfrak{p}$ regulär gibt es nun nach Hilfssatz 2 Nichtnullteiler $x_1, \ldots, x_s \in \mathfrak{p}$ mit $(x_1, \ldots, x_s)_\mathfrak{p} = \mathfrak{p} A_\mathfrak{p}$. Diese bilden also ein reguläres Parametersystem für $A_\mathfrak{p}$. Wir wenden nun die Induktionsvoraussetzung auf den Ring $\bar{A} = A/(x_s)$ und das Primideal $\bar{\mathfrak{p}} = \mathfrak{p}/(x_s)$ an. Da $x_s \in \mathfrak{r}(A)$ Nichtnullteiler von A war, ist $\bar{A}$ wieder ein semilokaler Cohen-Macaulay-Ring. Es ist $\bar{A}_{\bar{\mathfrak{p}}} = (A/(x_s))_{\bar{\mathfrak{p}}} \cong A_\mathfrak{p}/(x_s)_\mathfrak{p}$, also regulär und von der Dimension $s - 1$, da x_s regulärer Parameter von $A_\mathfrak{p}$ ist. Somit gibt es Elemente $\bar{a}_1, \ldots, \bar{a}_{s-1} \in \bar{\mathfrak{p}}$ mit $(\bar{a}_1, \ldots, \bar{a}_{s-1})_{\bar{\mathfrak{p}}} = \bar{\mathfrak{p}} \bar{A}_{\bar{\mathfrak{p}}}$ und $r(\bar{a}_1, \ldots, \bar{a}_{s-1}) = s - 1$. Für Elemente $a_i \in \bar{a}_i$ und $a_s = x_s$ aus A gilt dann $(a_1, \ldots, a_{s-1}, a_s)_\mathfrak{p} = (a_1, \ldots, a_{s-1})_\mathfrak{p} + (x_s)_\mathfrak{p} = \mathfrak{p} A_\mathfrak{p}$ und $r(a_1, \ldots, a_{s-1}, a_s) = s$ w. z. b. w.

Als unmittelbare Folgerung ergibt sich

Satz 2. *Ist A ein regulärer lokaler Ring, $\mathfrak{p} \subset A$ ein Primideal des Ranges $r(\mathfrak{p}) = s$, so gibt es s Elemente $a_1, \ldots, a_s \in \mathfrak{p}$ mit $(a_1, \ldots, a_s)_\mathfrak{p} = \mathfrak{p} A_\mathfrak{p}$ und $r(a_1, \ldots, a_s) = s$. $a_1, \ldots, a_s$ ist eine A-Folge.*

Zusatz. *Ist A lokal, so läßt sich das Elementsystem $a_1, \ldots, a_s$ in Satz 1 und 2 als Teil eines minimalen Erzeugendensystems des Primideals $\mathfrak{p}$ wählen.*

Beweis. Die Hilfssätze liefern, wie ihr Beweis zeigt, ein Elementsystem $x_1, \ldots, x_s$ mit den dortigen Eigenschaften, das Teil eines minimalen Erzeugendensystems von

$\mathfrak{p}$ ist. Insbesondere ist also mit $\mathfrak{m}$ als maximalem Ideal von A $x_s \notin \mathfrak{m}\,\mathfrak{p}$. Nun beweisen wir den Zusatz wie obigen Satz 1 durch Induktion nach s. Wie dort gibt es also hier Elemente $\bar{a}_1, \dots, \bar{a}_{s-1} \in \bar{\mathfrak{p}} \subset \bar{A}$ mit den dortigen Eigenschaften und der zusätzlichen Eigenschaft: $\bar{a}_1, \dots, \bar{a}_{s-1}$ ist Teil eines minimalen Erzeugendensystems von $\bar{\mathfrak{p}}$. Das wie dort gewählte Elementsystem $a_1, \dots, a_{s-1}, a_s$ ist nun auch Teil eines minimalen Erzeugendensystems von $\mathfrak{p}$: Aus $\alpha_1 a_1 + \cdots + \alpha_s a_s \in \mathfrak{m}\,\mathfrak{p}$, $\alpha_i \in A$, folgt nach Übergang zu $\bar{A}$

$$\bar{\alpha}_1 \bar{a}_1 + \cdots + \bar{\alpha}_{s-1} \bar{a}_{s-1} \in \bar{\mathfrak{m}}\,\bar{\mathfrak{p}},$$

also $\bar{\alpha}_i \in \bar{\mathfrak{m}}$ für $i = 1, \dots, s-1$. Daraus folgt $\alpha_i \in \mathfrak{m}$ und folglich $\alpha_s a_s = \alpha_s x_s \in \mathfrak{m}\,\mathfrak{p}$. Wäre nun α_s Einheit, so wäre $x_s \in \mathfrak{m}\,\mathfrak{p}$, entgegen $x_s \notin \mathfrak{m}\,\mathfrak{p}$. Also ist $\alpha_s \in \mathfrak{m}$, womit die Behauptung bewiesen ist.

Schließlich zeigen wir noch durch ein Beispiel[1]), daß in Hilfssatz 2 die Voraussetzung „A ist äquidimensional" notwendig ist: Wir geben einen lokalen Ring A mit einem Primideal $\mathfrak{p} \subset A$ vom Range $r(\mathfrak{p}) = 1$ an, so daß $A_{\mathfrak{p}}$ regulär ist und $\mathfrak{p}$ nur aus Nullteilern besteht. Dazu sei $R = k\,[[X, Y, Z, S, T]]$ ein freier Potenzreihenring über einem Körper k mit dem maximalen Ideal $\mathfrak{m}$ und $\mathfrak{a}$ das Ideal $\mathfrak{a} = \mathfrak{m}^3 \cap (SX + TY) \subset \subset (X, Y)$. Es ist $\mathfrak{m}^3$ primär zu $\mathfrak{m}$ und $(SX + TY)$ prim, ferner $(SX + TY) \notin \mathfrak{m}^3$, $\mathfrak{a}$ ist also in einer reduzierten Primärdarstellung gegeben. Wir setzen $A = R/\mathfrak{a}$, $\mathfrak{p} = = (X, Y)/\mathfrak{a}$. Dann ist $\mathfrak{p}$ ein Primideal und $r(\mathfrak{p}) \geqq 1$, da (X, Y) nicht zu $\mathfrak{a}$ assoziiert ist, also $\dim A_{\mathfrak{p}} \geqq 1$. Nun ist aber $\mathfrak{p} A_{\mathfrak{p}} = (\bar{X})$, denn $\mathfrak{p} = (X, Y)/\mathfrak{a} = (\bar{X}, \bar{Y})$ und $\bar{Z}\bar{S}\bar{X} + \bar{Z}\bar{T}\bar{Y} = 0$ in A, da $ZSX + ZTY \in \mathfrak{m}^3 \cap (SX + TY)$, also wegen $ZT \notin \notin (X, Y)$, d. h. $\bar{Z}\,\bar{T} \notin \mathfrak{p}$, $\bar{Y} = \dfrac{\bar{Z}\bar{S}}{\bar{Z}\bar{T}} \cdot \bar{X}$ in $A_{\mathfrak{p}}$. $A_{\mathfrak{p}}$ ist somit regulär von der Dimension 1. In A ist aber das maximale Ideal $\mathfrak{m}_A$ zu (0) assoziiert, da $\mathfrak{m}$ zu $\mathfrak{a}$ assoziiert war, $\mathfrak{p}$ besteht also aus lauter Nullteilern.

Ob in Satz 1 die Voraussetzung „A ist semilokaler Cohen-Macaulay-Ring" notwendig ist, wird durch dieses Beispiel nicht entschieden und bleibt offen.

Literaturverzeichnis

[1] M. Auslander and D. Buchsbaum, Codimension and multiplicity. Ann. of Math. 68, 625—657 (1958).

[2] W. Gröbner, Moderne algebraische Geometrie. Wien 1949.

[3] J. P. Serre, Multiplicites d'intersection. Cours au Collège de France 1957—1958 (vervielfältigt).

Eingegangen am 30. 11. 1960

Anschrift des Autors:

Hans-Joachim Nastold
Mathematisches Institut der Universität
Heidelberg, Tiergartenstraße

[1]) Dieses Beispiel wurde mir von Herrn R. Kiehl mitgeteilt.

Some Arithmetic Sums Connected with the Greatest Integer Function

By

L. CARLITZ

1. JACOBSTHAL [3] has defined the sum

$$S(a, b, m; r) = \sum_{k=0}^{r-1} D(k),$$

where

$$D(k) = D(a, b, m; k) = \left[\frac{a-b-k}{m}\right] - \left[\frac{a-k}{m}\right] - \left[\frac{b-k}{m}\right] + \left[\frac{k}{m}\right],$$

a and b are arbitrary integers while $m \geqq 1$, $r \geqq 1$. He proved that

(1) $$S(a, b, m; r) \geqq 0.$$

The writer [1] gave another proof of (1) by means of the representation

$$S(a, b, m; r) = -\frac{1}{m}\sum_{s=1}^{m-1}\frac{(\zeta^{-as}-1)(\zeta^{-bs}-1)(\zeta^{-cs}-1)}{(\zeta^{s}-1)(\zeta^{-s}-1)},$$

where $\zeta = e^{2\pi i/m}$. If we define

(2) $$J(a, b, c) = -\frac{1}{m}\sum_{s=1}^{m-1}\frac{(\zeta^{-as}-1)(\zeta^{-bs}-1)(\zeta^{-cs}-1)}{(\zeta^{s}-1)(\zeta^{-s}-1)}$$

then clearly $J(a, b, c)$ is symmetric in a, b, c and

$$S(a, b, m; r) = J(a, b, r).$$

It follows from (2) that

$$J(a, b, c) = J(-a, -b, -c)$$

and

$$J(a, b, c) = 0 \qquad (a\,b\,c = 0).$$

We may evidently assume without loss of generality that a, b, c (or $-a, -b, -c$) satisfy

(3) $$1 \leqq a \leqq m-1, \quad 1 \leqq b \leqq m-1, \quad 1 \leqq c \leqq m-1,$$

(4) $$b \leqq m - a \leqq c,$$

(5) $$b + c \leqq m.$$

When (3), (4), (5) hold, it is proved in [1] that

(6) $$J(a, b, c) = b.$$

In [2] the writer generalized the sum $S(a, b, m; r)$ in the following way. Let n be a fixed integer $\geqq 1$ and let $B_n(x)$ be the Bernoulli polynomial of degree n defined by

$$\frac{t e^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}. \tag{7}$$

Let $\bar{B}_n(x)$ be the Bernoulli function defined by

$$\bar{B}_n(x+1) = B_n(x) \quad (0 \leqq x \leqq 1), \qquad \bar{B}_n(x+1) = \bar{B}_n(x).$$

Now put

$$D_n(k) = D_n(a, b, m; k) = -\bar{B}_n\left(\frac{a+b+k}{m}\right) + \bar{B}_n\left(\frac{a+k}{m}\right) + \bar{B}_n\left(\frac{b+k}{m}\right) - \bar{B}_n\left(\frac{k}{m}\right),$$

$$S_n(a, b, m; r) = \sum_{k=0}^{r-1} D_n(k).$$

It is shown that

$$S_n(a, b, c; m) = -\frac{n}{m^n} \sum_{s=1}^{m-1} H_{n-1}(\zeta^{-s}) \frac{(\zeta^{-as} - 1)(\zeta^{-bs} - 1)(\zeta^{-cs} - 1)}{(\zeta^s - 1)(\zeta^{-s} - 1)},$$

where

$$\frac{1-\lambda}{e^t - \lambda} = \sum_{n=0}^{\infty} H_n(\lambda) \frac{t^n}{n!} \qquad (\lambda \neq 1). \tag{8}$$

Put

$$J_n(a, b, c) = -\frac{n}{m^n} \sum_{s=1}^{m-1} H_{n-1}(\zeta^{-s}) \frac{(\zeta^{-as} - 1)(\zeta^{-bs} - 1)(\zeta^{-cs} - 1)}{(\zeta^s - 1)(\zeta^{-s} - 1)}, \tag{9}$$

so that $J_n(a, b, c)$ is symmetric in a, b, c and has period m in each variable. We have also

$$S_n(a, b, m; r) = J_n(a, b, r), \qquad J(a, b, c) = J_1(a, b, c).$$

In [2] $J_2(a, b, c)$ is evaluated for $p = 2, 3$. It is found that if a, b, c satisfy (3), (4), (5), then

$$\frac{1}{2} m^2 J_2(a, b, c) = \frac{1}{2} m b (b-1) - b(m-a)(m-c), \tag{10}$$

$$\frac{1}{3} m^3 J_3(a, b, c) = \tag{11}$$
$$= \frac{1}{6} m b (b-1)(2b-1) - b(m-a)(m-c)(a-b-c-m-1).$$

In the present paper we evaluate $J_n(a, b, c)$ for arbitrary n. The general result is given in Theorem 1 below. Also some arithmetic properties of $J_n(a, b, c)$ are given in Theorems 2 and 3.

2. It is convenient to put

$$F(t) = F(a, b, c; t) = \sum_{n=1}^{\infty} J_n(a, b, c) \frac{(mt)^n}{n!}. \tag{12}$$

Then by (8) and (9)

$$
\begin{aligned}
F(t) &= -\sum_{s=1}^{m-1} \frac{(\zeta^{-as}-1)(\zeta^{-bs}-1)(\zeta^{-cs}-1)}{(\zeta^{s}-1)(\zeta^{-s}-1)} \cdot t \sum_{n=0}^{\infty} H_n(\zeta^{-s}) \frac{t^n}{n!} = \\
&= t \sum_{s-1}^{m-1} \frac{(\zeta^{-as}-1)(\zeta^{-bs}-1)(\zeta^{-cs}-1)}{(\zeta^{s}-1)(e^{t}-\zeta^{-s})}.
\end{aligned}
\tag{13}
$$

It follows from (13) that

$$
\begin{aligned}
F(-a,-b,-c;-t) &= -t \sum_{s=1}^{m-1} \frac{(\zeta^{-as}-1)(\zeta^{-bs}-1)(\zeta^{-cs}-1)}{(\zeta^{-s}-1)(e^{-t}-\zeta^{s})} = \\
&= -t\,e^{t} \sum_{s=1}^{m-1} \frac{(\zeta^{-as}-1)(\zeta^{-bs}-1)(\zeta^{-cs}-1)}{(\zeta^{s}-1)(e^{t}-\zeta^{-s})},
\end{aligned}
$$

so that

$$
F(-a,-b,-c;-t) = -e^{t} F(a,b,c;t). \tag{14}
$$

Thus by (12)

$$
m^n J_n(-a,-b,-c) = (-1)^{n-1} \sum_{s=1}^{n} \binom{n}{s} m^s J_s(a,b,c). \tag{15}
$$

Put

$$
\begin{aligned}
P(x) &= \sum_{s=1}^{m-1} \frac{(\zeta^{-as}-1)(\zeta^{-bs}-1)(\zeta^{-cs}-1)}{\zeta^{s}-1} \frac{x^m-1}{x-\zeta^{-s}} = \\
&= \sum_{s=0}^{m-1} (\zeta^{-bs}-1)(\zeta^{-cs}-1) \sum_{j=0}^{m-a-1} \zeta^{js} \sum_{k=1}^{m} x^{k-1} \zeta^{ks} = \\
&= \sum_{j=0}^{m-a-1} \sum_{k=1}^{m} x^{k-1} \sum_{s=0}^{m-1} \zeta^{(j+k)s} (\zeta^{-(b+c)s} - \zeta^{-bs} - \zeta^{-cs} + 1).
\end{aligned}
\tag{16}
$$

Since

$$
\sum_{s=0}^{m-1} \zeta^{rs} = \begin{cases} m & (m \mid r) \\ 0 & (m \nmid r), \end{cases}
$$

we get, using (3), (4), (5),

$$
\begin{aligned}
\frac{1}{m} \sum_{j=0}^{m-a-1} \sum_{k=1}^{m} x^{k-1} \sum_{s=0}^{m-1} \zeta^{(j+k-b-c)s} &= \frac{x^{b+c} - x^{a+b+c-m}}{x-1}, \\
\frac{1}{m} \sum_{j=0}^{m-a-1} \sum_{k=1}^{m} x^{k-1} \sum_{s=0}^{m-1} \zeta^{(j+k-b)s} &= \frac{x^{b}-1}{x-1} + \frac{x^m - x^{a+b}}{x-1}, \\
\frac{1}{m} \sum_{j=0}^{m-a-1} \sum_{k=1}^{m} x^{k-1} \sum_{s=0}^{m-1} \zeta^{(j+k-c)s} &= \frac{x^{c} - x^{a+c-m}}{x-1}, \\
\frac{1}{m} \sum_{j=0}^{m-a-1} \sum_{k=1}^{m} x^{k-1} \sum_{s=0}^{m-1} \zeta^{(j+k)s} &= \frac{x^{m} - x^{a}}{x-1}.
\end{aligned}
$$

It follows that

$$P(x) = \frac{x^{a+c-m}(x^m - 1)(x^b - 1) - (x^a - 1)(x^b - 1)(x^c - 1)}{x - 1};$$

hence in view of (13) and (16) we get

$$F(t) = \frac{mt}{e^t - 1} e^{(a+c-m)t}(e^{bt} - 1) - \frac{mt}{e^{mt} - 1} \frac{(e^{at} - 1)(e^{bt} - 1)(e^{ct} - 1)}{e^t - 1}. \tag{17}$$

3. If we use (7) it is clear that

$$\frac{mt}{e^t - 1} e^{(a-c-m)t}(e^{bt} - 1) = m \sum_{n=1}^{\infty} \{B_n(a + b + c - m) - B_n(a + c - m)\} \frac{t^n}{n!}. \tag{18}$$

The second term on the right of (17) can be handled in various ways. If we put

$$\frac{(e^{at} - 1)(e^{bt} - 1)(e^{ct} - 1)}{e^t - 1} = \sum_{n=2}^{\infty} f_n(a, b, c) \frac{t^n}{n!} \tag{19}$$

then it follows from (17) and (18) that

$$\begin{aligned} &m^n J_n(a, b, c) = \\ &= m\{B_n(a + b + c - m) - B_n(a + c - m)\} - \sum_{r=2}^{n} \binom{n}{r} m^{n-r} B_{n-r} f_r(a, b, c). \end{aligned} \tag{20}$$

It is easily verified that (19) implies

$$f_2(a, b, c) = 2abc, \quad f_3(a, b, c) = 3abc(a + b + c - 1),$$

$$f_4 = 2abc\{2(a^2 + b^2 + c^2) + 3(bc + ca + ab) - 3(a + b + c) + 1\}.$$

Hence (20) yields after a little computation

$$\begin{aligned} mJ_1(a, b, c) &= mb, \\ m^2 J_2(a, b, c) &= mb(b - 1) - 2b(m - a)(m - c), \\ m^3 J_3(a, b, c) &= \tfrac{1}{2} mb(b - 1)(2b - 1) - 3b(m - a)(m - c)(a - b - c - m - 1), \\ m^4 J_4(a, b, c) &= m(b(b - 1))^2 - b(m - a)(m - c)\{4(a^2 + b^2 + c^2) + \\ &\quad + 6(bc + ca + ab) - 6(m + 1)(a + b + c) - 2m(a + c - 3) + 4m^2 + 2\}, \end{aligned}$$

of which the first three are in agreement with (6), (10) and (11), respectively.

These special results suggest the possibility of a further transformation of (17). It is not difficult to verify that

$$F(t) = \frac{mt}{e^t - 1}(e^{bt} - 1) - \frac{mt\, e^{(a-c-m)t}}{e^{mt} - 1} \frac{(e^{(m-a)t} - 1)(e^{bt} - 1)(e^{(m-c)t} - 1)}{e^t - 1}. \tag{21}$$

Therefore we get, again using (19),

$$\begin{aligned} &m^n J_n(a, b, c) = \\ &= m\{B_n(b) - B_n\} - \sum_{r=2}^{n} \binom{n}{r} m^{n-r} B_{n-r}\left(\frac{a + c - m}{m}\right) f_r(m - a, b, m - c). \end{aligned} \tag{22}$$

For example, for $n = 3$, (22) becomes

$$m^3 J_3(a, b, c) = m\left(b^3 - \frac{3}{2} b^2 + \frac{1}{2} b\right) - 6m\left(\frac{a+c-m}{m} - \frac{1}{2}\right)(m-a)(m-c)\,b -$$
$$- 3b(m-a)(m-c)(2m-a-c+b-1) =$$
$$= \frac{1}{2} mb(b-1)(2b-1) - 3b(m-a)(m-c)(a+b+c-m-1)$$

as before.

From (19) it is evident that $f_n(a, b, c)$ is a polynomial in a, b, c with rational coefficients and of total degree $n + 1$. Indeed

$$f_n(a, b, c) = abc\,g_n(a, b, c), \tag{23}$$

where $g_n(a, b, c)$ is a polynomial with rational coefficients of total degree $n - 2$.

An explicit expression for $f_n(a, b, c)$ can be found as follows. Put

$$\frac{(e^{at}-1)(e^{bt}-1)(e^{ct}-1)}{e^t - 1} =$$
$$= \frac{1}{t}\frac{t}{e^t-1}\{e^{(a+b+c)t} - e^{(b+c)t} - e^{(c+a)t} - e^{(a+b)t} + e^{at} + e^{bt} + e^{ct} - 1\} =$$
$$= \frac{1}{t}\sum_{n=0}^{\infty}\frac{t^n}{n!}\{B_n(a+b+c) - B_n(b+c) - B_n(c+a) - B_n(a+b) +$$
$$+ B_n(a) + B_n(b) + B_n(c) - B_n\},$$

so that

$$f_n(a, b, c) = \frac{1}{n+1}\{B_{n+1}(a+b+c) - B_{n+1}(b+c) - B_{n+1}(c+a) - \tag{24}$$
$$- B_{n+1}(a+b) + B_{n+1}(a) + B_{n+1}(b) + B_{n+1}(c)\,B_{n+1}\}.$$

Since

$$\frac{1}{n+1}(B_{n+1}(a) - B_{n+1}) = \sum_{r=0}^{a-1} r^n = s_n(a),$$

(24) can also be written as

$$f_n(a, b, c) = s_n(a+b+c) - s_n(b+c) - s_n(c+a) - s_n(a+b) + s_n(a) + \tag{25}$$
$$+ s_n(b) + s_n(c).$$

We may now state

Theorem 1. *If a, b, c satisfy* (3), (4), (5), *$J_n(a, b, c)$ is evaluated by means of* (20) *and* (24). *Moreover $J_n(-a, -b, -c)$ is evaluated by means of* (15), (20) *and* (24).

Alternatively (22) may be used in place of (20) and (25) may be used in place of (24).

4. It is clear from (25) that $f_n(a, b, c)$ is an *integral-valued* polynomial in a, b, c. This is also an easy consequence of the following representation. Put

$$(e^{at}-1)(e^{ct}-1) = \sum_{n=2}^{\infty} C_n(a, c)\frac{t^n}{n!},$$

where

$$C_n(a, c) = (a+c)^n - a^n - c^n;$$

also put

$$\frac{e^{bt}-1}{e^t-1}=\sum_{n=0}^{\infty} s_n(b)\,\frac{t^n}{n!}\,,$$

where as above

$$s_n(b)=\sum_{r=0}^{b-1} r^n\,,\qquad s_0(b)=b\,.$$

Then

$$f_n(a,b,c)=\sum_{r=2}^{n}\binom{n}{r} C_r(a,c)\,s_{n-r}(b)\,. \tag{26}$$

From (26) we see that $f_n(a, b, c)$ *is a polynomial in a and c with coefficients that are integral-valued polynomials in b*. We may of course cyclically permute a, b, c in this statement.

For n prime (26) reduces to

$$f_n(a,b,c)\equiv C_n(a,c)\,s_0(b)\equiv((a+c)^n-a^n-c^n)\,b \pmod n\,,$$

so that

$$f_p(a,b,c)\equiv 0 \pmod p \quad (p \text{ prime})\,. \tag{27}$$

In this case one can easily show that each coefficient in $f_p(a, b, c)$ is divisible by p.

We recall that

$$B_n(x)=\sum_{r=0}^{n}\binom{n}{r} B_{n-r}\,x^r\,,$$

so that (24) becomes

$$f_n(a,b,c)=\frac{1}{n+1}\sum_{r=3}^{n+1}\binom{n+1}{r} B_{n+1-r}\,u_r(a,b,c)\,, \tag{28}$$

where

$$u_n(a,b,c)=(a+b+c)^n-(b+c)^n-(c+a)^n-(a+b)^n+a^n+b^n+c^n\,.$$

Clearly the polynomial $u_n(a, b, c)$ is divisible by abc. In particular $u_3(a, b, c) = 6abc$. Thus the term of lowest degree in the right member of (28) reduces to

$$n(n-1)\,B_{n-2}\,. \tag{29}$$

Now let p be a prime $\geqq 3$ and take $n = 3p - 1$. Since $p-1 \mid n-2$ it follows from the Staudt-Clausen theorem that the denomiator of B_{n-2} is divisible by p. On the other hand

$$n(n-1)=(2p-1)(3p-2)\not\equiv 0 \pmod p\,.$$

Consequently the product in (29) is not integral. We conclude that *the coefficients of* $f_n(a, b, c)$ *are not necessarily integral*. Thus the first few values are misleading in this respect.

5. Returning to $J_n(a, b, c)$, it is obvious from the definition that $J_n(a, b, c)$ is rational for all integral a, b, c. This can be made more precise. We have by (9)

$$\frac{m^n}{n} J_n(a, b, c) = -\sum_{s=1}^{m-1} H_{n-1}(\zeta^{-s}) \frac{(\zeta^{-as}-1)(\zeta^{-bs}-1)(\zeta^{-cs}-1)}{(\zeta^s-1)(\zeta^{-s}-1)}.$$

Also

$$H_n(x) = \frac{A_n(x)}{(x-1)^n},$$

where $A_n(x)$ is a polynomial with integral coefficients.

In the cyclotomic field $R(\zeta)$, it is familiar that when m is divisible by at least two distinct primes, $1-\zeta$ is a unit, while if $m = p^r$, where p is prime, then $1-\zeta \mid p$.

This proves

Theorem 2. *If m is divisible by at least two distinct primes, then*

$$\frac{m^n}{n} J_n(a, b, c)$$

is integral for all a, b, c, n. If $m = p^r$, where p is a prime, then there exists an integer N depending on n such that

$$\frac{m^N}{n} J_n(a, b, c)$$

is integral for all a, b, c, n.

In the next place, if $m = p^r$ and a, b, c satisfy (3), (4), (5), then by (20)

$$\frac{m^n}{n} J_n(a, b, c) = \frac{m}{n}\{B_n(a+b+c-m) - B_n(a+c-m)\} -$$
$$-\sum_{s=1}^{n-2} \binom{n-1}{s-1} \frac{m^s B_s}{s} f_{m-s}(a, b, c) - \frac{1}{n} f_n(a, b, c).$$

Now

$$\frac{1}{n}\{B_n(a+b+c-m) - B_n(a+c-m)\}$$

is integral. If $p-1 \mid s$ and also $p^k \mid s$, then $s \geqq k+1$ and it follows that $m^s B_s/s$ is integral $(\bmod\, p)$; the same conclusion holds when s is not divisible by $p-1$. Consequently

$$\frac{m^n}{n} J_n(a, b, c) + \frac{1}{n} f_n(a, b, c)$$

is integral $(\bmod\, p)$. Also by (15)

$$\frac{m^n}{n} J_n(-a, -b, -c) = (-1)^{n-1} \sum_{s=1}^{n} \binom{n-1}{s-1} \left\{\frac{m^s}{s} J_s(a, b, c) + \frac{1}{s} f_s(a, b, c)\right\} +$$
$$+ \frac{(-1)^n}{n} \sum_{s=2}^{n} \binom{n}{s} f_s(a, b, c).$$

By (19) we get

$$\sum_{n=2}^{\infty} f_n(-a, -b, -c) \frac{(-t)^n}{n!} = -e^t \sum_{n=2}^{\infty} f_n(a, b, c) \frac{t^n}{n!},$$

so that

$$f_n(-a, -b, -c) = (-1)^{n-1} \sum_{s=2}^{n} \binom{n}{s} f_s(a, b, c).$$

Therefore

$$\frac{m^n}{n} J_n(-a, -b, -c) + f_n(-a, -b, -c) =$$

$$= (-1)^{n-1} \sum_{s=1}^{n} \binom{n-1}{s-1} \left\{ \frac{m^s}{s} J_s(a, b, c) + \frac{1}{s} f_s(a, b, c) \right\}.$$

This proves

Theorem 3. *If $m = p^r$, where p is a prime, then*

$$\frac{m^n}{n} J_n(a, b, c) + \frac{1}{n} f_n(a, b, c)$$

is integral for all a, b, c, n. In particular if $n = p$, then

$$\frac{m^n}{n} J_n(a, b, c)$$

is integral for all a, b, c.

The last statement follows from (27).

It would be of interest to know something about the fractional part of $f_n(a, b, c)/n$ for arbitrary n. By (25) we get

(30) $$f_{pn}(a, b, c) \equiv f_n(a, b, c) \pmod{p},$$

where p is an arbitrary prime. In particular (30) contains

$$f_p(a, b, c) \equiv 0 \pmod{p},$$

$$f_{2p}(a, b, c) \equiv 2abc \pmod{p},$$

$$f_{3p}(a, b, c) \equiv 3abc(a + b + c - 1) \pmod{p}$$

and so on. It is also evident from (25) that

(31) $$f_{p^r n}(a, b, c) \equiv f_{p^{r-1} n}(a, b, c) \pmod{p^r},$$

where $r \geqq 1$ and n is arbitrary.

We note also that (25) implies

$$f_{n+p-1}(a, b, c) \equiv f_n(a, b, c) \pmod{p}$$

and more generally

$$\sum_{s=0}^{r}(-1)^{s}\binom{r}{s}f_{n+s+p-1}(a,b,c)\equiv 0 \pmod{p^{r}} \tag{32}$$

for all $n \geq r \geq 1$.

We have tacitly assumed in deriving (30), (31), (32) that a, b, c are non-negative. However it is not difficult to see that this assumption is superfluous.

References

[1] L. CARLITZ, An arithmetic sum connected with the greatest integer function. Norske Vid. Selsk. Forhdl. Trondheim **32**, 24—30 (1959).

[2] L. CARLITZ, Some arithmetic sums connected with the greatest integer function. Mathematica Scandinavica **8**, 59—64 (1960).

[3] E. JACOBSTHAL, Über eine zahlentheoretische Summe. Norske Vid. Selsk. Forhdl. Trondheim **30**, 35—41 (1957).

Eingegangen am 28. 8. 1960

Anschrift des Autors:

L. Carlitz
Department of Mathematics
Duke University
Durham (N. C.), USA

Eine Bemerkung zur Werteverteilung meromorpher Funktionen in der Halbebene

Von

Klaus Habetha

1. Einleitung. Bei der Untersuchung der Werteverteilung von in einer Halbebene meromorphen Funktionen $w(z)$ (s. dazu Nevalinna [6][1]), Dufresnoy [4]) treten im 2. Hauptsatz im Restglied Integrale über den Rand der Halbebene auf, die durch eine Abschätzung der logarithmischen Ableitung von $w(z)$ weiter untersucht werden. Dazu muß die Charakteristik bezüglich eines etwas größeren Winkelraumes herangezogen werden.

In dieser Arbeit soll eine Möglichkeit gezeigt werden, diesen Weg durch Einführung anderer Charakteristiken zu umgehen. Man behandelt damit das Problem einerseits ganz in der Halbebene und kann andererseits die Ahlforssche Methode [1] zur Abschätzung des Restgliedes verwenden. In letzterem kommt es dann auf das relative Wachstum zweier dieser Charakteristiken an. Darin macht sich natürlich implizit der Einfluß der Randwerte bemerkbar. — Die gleichen Rechnungen lassen sich in allgemeineren Winkelräumen $\left\{z \,\middle|\, |\arg z| < \frac{\pi}{2k}\right\}$ durchführen.

2. Der 1. Hauptsatz. Für das folgende wird eine Formel von F. und R. Nevanlinna [5] zugrunde gelegt (s. auch Dinghas [2]): für ein Gebiet G endlichen Zusammenhangs mit stückweise stetig gekrümmtem Rand ∂G gilt

$$\sum_{\nu} \lambda(a_\nu) - \sum_{\mu} \lambda(b_\mu) = \frac{1}{2\pi} \int_G \log|w(z)|\, \Delta\lambda\, d\sigma + \frac{1}{2\pi} \int_{\partial G} \left(\log|w| \frac{\partial \lambda}{\partial n} - \lambda \frac{\partial}{\partial n} \log|w|\right) ds\,.$$

Dabei sei $d\sigma$ das Flächenelement von G, ds das Bogenelement von ∂G und $\partial/\partial n$ die Ableitung nach der inneren Normalen von ∂G. Ferner sei $w(z)$ in $G \cup \partial G$ eindeutig und meromorph sowie $\lambda(z)$ dort zweimal stetig differenzierbar. Die Summen links sind über die Null- bzw. Polstellen von $w(z)$ in G zu erstrecken, jeweils mit entsprechender Vielfachheit gezählt.

Sei nun G_{r/r_0} der Halbkreisring

(2.1) $$G_{r/r_0} = \left\{z \,\middle|\, 0 < r_0 < |z| < r;\ |\arg z| < \frac{\pi}{2}\right\},$$

sowie

(2.2) $$\Gamma_r = \left\{z \,\middle|\, |z| = r;\ |\arg z| \leqq \frac{\pi}{2}\right\}.$$

[1]) Zahlen in eckigen Klammern verweisen auf das Literaturverzeichnis am Ende der Arbeit.

$w(z)$ sei in

$$\left\{ z \,|\, r_0 \leq |z| \,;\, |\arg z| \leq \frac{\pi}{2} \right\}$$

meromorph und man setze $\lambda(z) = x^l$ ($x = \operatorname{Re}(z)$; $l > 0$, ganz). Für $w(z) \neq a, b$ auf Γ_r und Γ_{r_0} ($a, b \neq \infty$) ergibt sich

$$(2.3)\qquad \begin{aligned} \sum_{\substack{w(z_\nu)=a \\ z_\nu \in G_{r/r_0}}} x_\nu^l - \sum_{\substack{w(z_\mu)=b \\ z_\mu \in G_{r/r_0}}} x_\mu^l = \frac{l(l-1)}{2\pi} \int_G \log \left| \frac{w(z)-a}{w(z)-b} \right| x^{l-2}\, d\sigma + \\ + \frac{\delta_{1l}}{2\pi} \int_{r_0}^{r} \log \left\{ \left| \frac{w(it)-a}{w(it)-b} \right| \left| \frac{w(-it)-a}{w(-it)-b} \right| \right\} dt + \\ + \frac{1}{2\pi} \int_{\Gamma_r - \Gamma_{r_0}} \left\{ -l \log \left| \frac{w-a}{w-b} \right| + r \frac{\partial}{\partial r} \log \left| \frac{w-a}{w-b} \right| \right\} r^l \cos^l \varphi \, d\varphi\, . \end{aligned}$$

Dabei sei δ_{1l} das Kroneckersche Symbol. Die a- bzw. b-Stellen auf der y-Achse kann man durch einen üblichen Grenzübergang behandeln. Führt man die Bezeichnungen

$$(2.4)\qquad n_l(r, a) = \sum_{\substack{w(z_\nu)=a \\ z_\nu \in G_{r/r_0}}} x_\nu^l\,,$$

$$(2.5)\qquad m_l(r, a) = \frac{1}{2\pi r^l} \int_{\Gamma_r} \log \frac{1}{[w, a]} \cos^l \varphi \, d\varphi \quad \left([w, a] = \frac{|w-a|}{\sqrt{1+|w|^2}\sqrt{1+|a|^2}} \right)$$

und

$$(2.6)\qquad \mu(r, a) = \frac{1}{2\pi} \int_{r_0}^{r} \frac{dt}{t^3} \int_{r_0}^{t} \log \frac{1}{[w(i\tau), a]\,[w(-i\tau), a]}\, d\tau$$

ein, so folgt aus (2.3), daß die Größe

$$(2.7)\qquad \begin{aligned} S_l(r) = n_l(r, a) + r^{2l+1} m_l'(r, a) + \delta_{1l} r^3 \mu'(r, a) + \\ + l(l-1) \int_{r_0}^{r} t^{2l-3} m_{l-2}(t, a)\, dt - r_0^{2l+1} m_l'(r_0, a) \end{aligned}$$

von a unabhängig ist. Man zeigt sofort aus (2.3) mit

$$w(z) \text{ an Stelle von } (w(z)-a)/(w(z)-b),$$

daß in (2.7) auch $a = \infty$ zulässig ist. Bei Integration von r_0 bis r erhält man mit

$$(2.8)\qquad N_l(r, a) = \int_{r_0}^{r} \frac{n_l(t, a)}{t^{2l+1}}\, dt$$

und

$$(2.9)\qquad T_l(r, a) = \int_{r_0}^{r} \frac{S_l(t)}{t^{2l+1}}\, dt$$

den ersten Hauptsatz in der Gestalt:

Die Größe

$$T_l(r) = N_l(r,a) + m_l(r,a) + \frac{l-1}{2}\int_{r_0}^{r} t^{2l-3}\left(\frac{1}{t^{2l}} - \frac{1}{r^{2l}}\right) m_{l-2}(t,a)\,dt + \tag{2.10}$$
$$+ \delta_{1l}\,\mu(r,a) - m_l(r_0,a) - \frac{r_0 m_l'(r_0,a)}{2l}\left(1 - \frac{r_0^{2l}}{r^{2l}}\right)$$

ist von a unabhängig, solange auf Γ_{r_0} überall $w(z) \neq a$ ist.

Die Bedingung $w(z) \neq a$ auf Γ_r kann wegen der Stetigkeit (in r) der Summanden in (2.10) weggelassen werden. In (2.10) tritt nun ein Glied mit Randwerten von $w(z)$ nur für den bisher behandelten Fall $l = 1$ auf, für $l > 1$ hat man dafür das Integral über $m_{l-2}(r,a)$.

Die Integraldarstellung von $T_l(r)$ nach Shimizu-Ahlfors ist auch hier möglich: Bei Multiplikation von (2.10) mit dem sphärischen Flächenelement

$$d\omega(a) = \frac{|a|\,d|a|\,d\alpha}{(1+|a|^2)^2} \qquad (a = |a|\,e^{i\alpha})$$

und Integration über die a-Ebene E erhält man

$$T_l(r) = \frac{1}{\pi}\int_{r_0}^{r}\frac{dt}{t^{2l+1}}\int_E n_l(t,a)\,d\omega(a) + \frac{1}{8\pi}\left(\frac{r_0^l}{r^{2l}} - \frac{1}{r_0^l}\right)\int_{-\pi/2}^{\pi/2}\cos^l\varphi\,d\varphi - \tag{2.11}$$
$$- \frac{r_0}{2l\pi}\left(1 - \frac{r_0^{2l}}{r^{2l}}\right)\int_E m'(r_0,a)\,d\omega(a)\,.$$

Dabei ist die Gleichung

$$\int_E \log\frac{1}{[w,a]}\,d\omega(a) = \frac{\pi}{2}$$

(unabhängig von w) berücksichtigt worden. Das letzte Integral in (2.11) ist endlich, denn bis auf die Menge

$$E_0 = \{a \,|\, w(z) = a, z \in \Gamma_{r_0}\}$$

vom Flächenmaß 0 ist $m_l'(r_0,a)$ nach (2.10) gleich einer über a integrierbaren Funktion, also selbst integrierbar. Schließlich erhält man aus (2.11) und der Beziehung

$$\int_E n_l(t,a)\,d\omega(a) = \int_{G_{t/r_0}} x^l\,\frac{|w'|^2}{(1+|w|^2)^2}\,d\sigma$$

$$T_l(r) = \frac{1}{\pi}\int_{r_0}^{r}\frac{dt}{t^{2l+1}}\int_{G_{t/r_0}} x^l\,\frac{|w'|^2}{(1+|w|^2)^2}\,d\sigma + \frac{C_0}{r^{2l}} + C_1 \qquad (C_0, C_1 = \text{const.})\,. \tag{2.12}$$

Das ist die Integraldarstellung von $T_l(r)$, aus ihr folgt z. B. die Konvexität von $T_l(r)$ als Funktion von r^{-2l}.

Für die Abschätzung des Restgliedes im 2. Hauptsatz wird nach Ahlfors noch eine Ungleichung benötigt. Dazu seien $a_1, \ldots, a_q$ verschiedene komplexe Zahlen

und

$$\varrho(a) = C\Pi^{-2}\log^{-2}\Pi \quad \left(\Pi = \prod_{\nu=1}^{q}[a, a_\nu]\right). \tag{2.13}$$

Die Konstante C werde so bestimmt, daß

$$\int_E \varrho(a)\, d\omega(a) = 1$$

gilt. Dieses Integral existiert im Lesbesgueschen Sinne. Nun ergibt sich aus (2.10) die Ungleichung

$$T_l(r) \geqq N_l(r, a) - m_l(r_0, a) - \frac{r_0}{2l}\left(1 - \frac{r_0^{2l}}{r^{2l}}\right) m_l'(r_0, a). \tag{2.14}$$

Nimmt $w(z)$ auf Γ_{r_0} die Zahlen $a_1, \ldots, a_q$ nicht an, so ist

$$\operatorname*{Min}_{\substack{\nu=1,\ldots,q\\ z\in\Gamma_{r_0}}} [w(z), a_\nu] = \delta > 0$$

und die Integrale

$$\int_E \varrho(a)\log\frac{1}{[w,a]}\, d\omega(a), \qquad \int_E \varrho(a)\frac{d\omega(a)}{[w,a]}$$

existieren und lassen sich durch nur von δ und den a_ν abhängige Konstanten abschätzen. Auf Grund der Ungleichung

$$\left|\frac{\partial}{\partial r}\log\frac{1}{[w,a]}\right| \leqq \frac{|w'|}{(1+|w|^2)\,[w,a]}$$

(s. Dinghas [3], S. 398) ergibt dann aber

$$\int_E \varrho(a)\, m_l'(r_0, a)\, d\omega(a)$$

eine endliche Zahl, in die natürlich die Werte von $w(z)$ auf Γ_{r_0} eingehen. Multipliziert man jetzt (2.14) mit $\varrho(a)\,d\omega(a)$ und integriert über E, so folgt

$$T_l(r) \geqq \int_{r_0}^{r}\frac{dt}{t^{2l+1}}\int_{G_{t/r_0}} x^l\,\varrho(w)\frac{|w'|^2}{(1+|w|^2)^2}\,d\sigma + \text{const}. \tag{2.15}$$

Setzt man zur Abkürzung

$$S_{\varrho l}(r) = \int_{G_{r/r_0}} x^l\,\varrho(w)\frac{|w'|^2}{(1+|w|^2)^2}\,d\sigma \tag{2.16}$$

und

$$T_{\varrho l}(r) = \int_{r_0}^{r}\frac{S_{\varrho l}(t)}{t^{2l+1}}\,dt, \tag{2.17}$$

so schreibt sich (2.15) in der Form

$$T_l(r) \geqq T_{\varrho l}(r) + \text{const}. \tag{2.18}$$

3. Der 2. Hauptsatz. Für das Folgende werde angenommen, daß $a_1, \ldots, a_q (q > 2)$ verschiedene komplexe Zahlen sind und daß $w(z)$ auf Γ_{r_0} diese Werte nicht annimmt, ebenso sei dort $w'(z) \neq 0, \infty$. Das bedeutet keine Einschränkung der Allgemeinheit, da man gegebenenfalls nur r_0 zu ändern braucht.

Man bilde die Größe

$$N_{1l}(r) = 2 N_l(r, \infty) - N_l'(r, \infty) + N_l'(r, 0), \tag{3.1}$$

dabei beziehen sich die mit einem Strich versehenen Größen auf $w'(z)$. $N_{1l}(r)$ zählt wie üblich alle mehrfachen Stellen von $w(z)$ mit um 1 verminderter Vielfachheit. Aus (2.10) ergibt sich nun

$$\begin{aligned}(q-2)\, T_l(r) = \sum_{\nu=1}^{q} N_l(r, a_\nu) - N_{1l}(r) + \frac{1}{2\pi r^l}\int_{\Gamma_r} \log \Phi \cos^l \varphi \, d\varphi \, + \\ + \frac{l-1}{2}\int_{r_0}^{r} t^{2l-3}\left(\frac{1}{t^{2l}} - \frac{1}{r^{2l}}\right)\frac{1}{2\pi t^{l-2}}\int_{\Gamma_t} \log \Phi \cos^{l-2}\varphi \, d\varphi \, dt \, + \\ + \frac{\delta_{1l}}{2\pi}\int_{r_0}^{r}\frac{dt}{t^3}\int_{r_0}^{t} \log\{\Phi(i\tau)\,\Phi(-i\tau)\}\, d\tau + O(1),\end{aligned} \tag{3.2}$$

wobei

$$\Phi(z) = \frac{|w'|}{1+|w|^2}\prod_{\nu=1}^{q}\frac{1}{[w, a_\nu]} \tag{3.3}$$

gesetzt ist. Von jetzt an werde angenommen, daß $l > 2$ ist, dann fällt in (3.2) das Glied mit den Randwerten fort. Zu untersuchen bleiben die Integrale

$$I_l = \frac{1}{2\pi r^l}\int_{\Gamma_r} \log \Phi \cos^l \varphi \, d\varphi . \tag{3.4}$$

Aus (2.13) erhält man

$$I_l = \frac{1}{4\pi r^l}\int_{\Gamma_r}\left\{\log\left(\frac{|w'|^2}{(1+|w|^2)^2}\,\varrho(w)\right) + \log\left(\frac{1}{C}\log^2\left(\prod_{\nu=1}^{q}\frac{1}{[w, a_\nu]}\right)\right)\right\}\cos^l\varphi \, d\varphi . \tag{3.5}$$

Nun gilt der

Hilfssatz 1. *Auf der meßbaren Menge Δ seien $f(x)$ und $g(x)$ nicht negativ, nicht identisch Null und $g(x)$, $f(x)$ sowie $\log f(x)$ seien quadratisch integrierbar. Dann ist*

$$\frac{1}{C}\int_{\Delta} g(x)\log f(x)\, dx \leqq \log\left\{\frac{1}{C}\int_{\Delta} g(x)\, f(x)\, dx\right\} \qquad \left(C = \int_{\Delta} g(x)\, dx\right).$$

Der Beweis folgt sofort aus der Ungleichung $\log(1+x) \leqq x$ $(x \geqq -1)$, wenn man $f(x) = m + \delta$ setzt mit

$$m = \frac{1}{C}\int_{\Delta} f(x)\, g(x)\, dx .$$

Damit kann man aus (3.5) für die r, für die $w(z) \neq a_1, \ldots, a_q$ auf Γ_r ist,

$$(3.6)\quad \begin{aligned} I_l \leqq \frac{\gamma_l}{4\pi r^l} \log\left(\frac{1}{\gamma_l}\int_{\Gamma_r} \frac{|w'|^2}{(1+|w|^2)^2}\,\varrho(w)\cos^l\varphi\,d\varphi\right) + \\ + \frac{\gamma_l}{2\pi r^l}\log\left(\frac{1}{\gamma_l}\int_{\Gamma_r}\log\left\{\prod_{\nu=1}^{q}\frac{1}{[w,a_\nu]}\right\}\cos^l\varphi\,d\varphi\right) + O(1) \end{aligned}$$

ableiten (es ist

$$\gamma_l = \int_{-\pi/2}^{\pi/2} \cos^l\varphi\,d\varphi$$

gesetzt). Aus (2.10) erhält man

$$m_l(r,a) \leqq T_l(r) + O(1)$$

und aus (2.16)

$$S'_{\varrho l}(r) = r^{l+1}\int_{\Gamma_r}\frac{|w'|^2}{(1+|w|^2)^2}\,\varrho(w)\cos^l\varphi\,d\varphi$$

(bis auf die oben ausgeschlossenen r), das ergibt

$$(3.7)\quad \begin{aligned} I_l &\leqq \frac{\gamma_l}{4\pi r^l}\log\frac{S'_{\varrho l}(r)}{r^{l+1}} + \frac{\gamma_l}{2\pi r^l}\log\{q\,T_l(r) + O(1)\} + O(1) \leqq \\ &\leqq \frac{\gamma_l}{4\pi r^l}\log S'_{\varrho l}(r) + O\left(1 + \frac{\log T_l(r)}{r^l}\right). \end{aligned}$$

Nun muß ein zweiter, ebenfalls bekannter Hilfssatz herangezogen werden:

Hilfssatz 2. *Für $x \geqq x_0$ sei $g(x) > 0$, stetig, monoton wachsend und bis auf isolierte Punkte differenzierbar, dann ist das Maß der Menge*

$$E_x = \{x \mid g'(x) > g^2(x);\, x \geqq x_0\}$$

nach oben beschränkt.

Der Beweis folgt aus

$$\int_{E_x} dx \leqq \int_{E_x} g^{-2}\,dg < \infty\,.$$

Danach ist also bis auf eine r-Menge endlichen Maßes

$$I_l \leqq \frac{\gamma_l}{2\pi r^l}\log S_{\varrho l}(r) + O\left(1 + \frac{\log T_l(r)}{r^l}\right).$$

Eine nochmalige Anwendung des Hilfssatzes 2 und der Ungleichung (2.18) liefert

$$(3.8)\quad I_l \leqq O\left(1 + \frac{\log T_l(r)}{r^l}\right),$$

gleichfalls bis auf eine Menge Δ von endlichem Maß. Damit erhält man aus (3.2) $(l > 2)$

(3.9)
$$(q-2)\,T_l(r) < \sum_{\nu=1}^{q} N_l(r,a_\nu) - N_{1l}(r) + O\left(1+\frac{\log T_l(r)}{r^l}\right) + \\ + \frac{l-1}{2}\int_{r_0}^{r} t^{2l-3}\left(\frac{1}{t^{2l}}-\frac{1}{r^{2l}}\right) I_{l-2}(t)\,dt\,.$$

Das letzte Integral J_l kann man in der Form schreiben:

$$J_l = l(l-1)\int_{r_0}^{r}\frac{dt}{t^{2l+1}}\int_{r_0}^{t}\tau^{2l-3} I_{l-2}(\tau)\,d\tau\,.$$

Setzt man hier (3.7) ein, so ergibt sich

$$J_l \leqq l(l-1)\int_{r_0}^{r}\frac{dt}{t^{2l+1}}\int_{r_0}^{t}\tau^{2l-3}\left\{\frac{\gamma_{l-2}}{4\pi\tau^{l-2}}\log S'_{\varrho(l-2)}(\tau) + O\left(1+\frac{\log T_{l-2}(\tau)}{\tau^{l-2}}\right)\right\}d\tau$$

und weiter

$$J_l \leqq O\left(\int_{r_0}^{r}\frac{\log T_{l-2}(t)}{t^{l+1}}\,dt\right) + \frac{l(l-1)\gamma_{l-2}}{4\pi}\int_{r_0}^{r}\frac{dt}{t^{2l+1}}\int_{r_0}^{t}\tau^{l-1}\log S'_{\varrho(l-2)}(\tau)\,d\tau\,.$$

Wendet man Hilfssatz 1 auf das letzte Integral an, so folgt

$$J_l \leqq O\left(\int_{r_0}^{r}\frac{\log T_{l-2}(t)}{t^{l+1}}\,dt\right) + \frac{(l-1)\gamma_{l-2}}{4\pi}\int_{r_0}^{r}\frac{t^l-r_0^l}{t^{2l+1}}\log\left\{\int_{r_0}^{t}\tau^{l-1} S'_{\varrho(l-2)}(\tau)\,d\tau\right\}dt \leqq$$

$$\leqq O\left(\int_{r_0}^{r}\frac{\log T_{l-2}(t)}{t^{l+1}}\,dt\right) + \frac{(l-1)\gamma_{l-2}}{4\pi}\int_{r_0}^{r}\frac{1}{t^{l+1}}\log\{t^{l-1} S_{\varrho(l-2)}(t)\}\,dt\,.$$

Aus

$$T'_{\varrho(l-2)} = (\log T_{\varrho(l-2)})'\,T_{\varrho(l-2)}$$

schließt man

$$J_l \leqq O\left(\int_{r_0}^{r}\frac{\log T_{l-2}(t)}{t^{l+1}}\,dt\right) + O\left(\log\left\{\int_{r_0}^{r}\frac{(\log T_{\varrho(l-2)}(t))'}{t^{l+1}}\,dt\right\}\right) \leqq$$

$$\leqq O\left(\int_{r_0}^{r}\frac{\log T_{l-2}(t)}{t^{l+1}}\,dt\right) + O\left(\log\left\{\frac{\log T_{\varrho(l-2)}(r)}{r^{l+1}}\right\}\right).$$

Nach Hilfssatz 2 ist bis auf eine Menge von r-Werten endlichen Maßes

$$\frac{\log T_{\varrho(l-2)}(r)}{r^{l+1}} \leqq \left(\int_{r_0}^{r}\frac{\log T_{\varrho(l-2)}(t)}{t^{l+1}}\,dt\right)^2,$$

damit folgt schließlich (immer unter Berücksichtigung von (2.18))

(3.10)
$$J_l \leqq O\left(\int_{r_0}^{r}\frac{\log T_{l-2}(t)}{t^{l+1}}\,dt\right).$$

Aus (3.9) und (3.10) erhält man nun den 2. Hauptsatz in der folgenden Form:

Satz. *$w(z)$ sei für $\{z \mid |z| \geq r_0;\ |\arg z| \leq \pi/2\}$ meromorph. $a_1, \ldots, a_q$ seien verschiedene komplexe Zahlen und auf $\{z \mid |z| = r_0;\ |\arg z| \leq \pi/2\}$ sei $w(z) \neq a_1, \ldots, a_q$ sowie $w'(z) \neq 0, \infty$. Definiert man $T_l(r)$ durch* (2.12), *$N_l(r)$ durch* (2.8) *und $N_{1l}(r)$ durch* (3.1), *so gilt für $l > 2$ bis auf eine Menge von r-Werten von endlichem Maß*

$$(q-2)\, T_l(r) \leq \sum_{\nu=1}^{q} N_l(r, a_\nu) - N_{1l}(r) + O\left(\frac{\log T_l(r)}{r^l} + \int_{r_0}^{r} \frac{\log T_{l-2}(t)}{t^{l+1}}\, dt\right).$$

Literaturverzeichnis

[1] L. AHLFORS, Über eine Methode in der Theorie der meromorphen Funktionen. Soc. Sci. Fenn., Comm. Phys.-Math. **8**, Nr. 10 (1935).

[2] A. DINGHAS, Bemerkungen zur Ahlforsschen Methode in der Theorie der meromorphen Funktionen I. Comp. Math. **5**, 107–118 (1937).

[3] A. DINGHAS, Zum Verhalten eindeutiger analytischer Funktionen in der Umgebung einer wesentlichen isolierten Singularität. Math. Z. **66**, 389–408 (1957).

[4] J. DUFRESNOY, Sur les fonctions dans un angle. C. R. Acad. Sci. Paris **208**, 718–720 (1939).

[5] F. und R. NEVANLINNA, Über die Eigenschaften analytischer Funktionen in der Umgebung einer singulären Stelle oder Linie. Acta Soc. Sci. Fenn. **50**, Nr. 5 (1922).

[6] R. NEVANLINNA, Über die Eigenschaften meromorpher Funktionen in einem Winkelraum. Acta Soc. Sci. Fenn. **50**, Nr. 12 (1925).

Eingegangen am 20. 6. 1960

Anschrift des Autors:

Klaus Habetha
Berlin-Charlottenburg
Hardenbergstr. 24

Über das Koeffizientenproblem der rationalen Funktionen mit positivem Realteil

Von

F. H. Effertz und W. Meuffels

Einleitung. Eine rationale Funktion $f(z)$ mit reellen Koeffizienten bezeichnet man als positiv reelle rationale Funktion (abgekürzt p. r. Funktion), wenn sie
a) in der offenen rechten Halbebene $\operatorname{Re} z > 0$ regulär ist und
b) dort positiven Realteil besitzt.

Die Zugehörigkeit einer beliebig vorgegebenen rationalen Funktion der Form

(1) $$f(z) = \frac{C(z)}{A(z)}$$

mit

$$C(z) = c_0 z^m + c_1 z^{m-1} + \cdots + c_m, \quad c_0 \neq 0,$$

und

$$A(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n, \quad a_0 \neq 0,$$

$$\operatorname{Max}(m, n) \geqq 1, \quad c_i, \quad a_i \quad \text{reell},$$

zur Klasse der p. r. Funktionen kann mit Hilfe von rekursiven Verfahren stets nachgewiesen werden [1]. Diese rekursiven Methoden, welche meist einen beträchtlichen Rechenaufwand erfordern, ergeben sich aus den Charakterisierungen der p. r. Funktionen von O. Brune [2] und H. Piloty [3]:

1. Die Brunebedingungen für p. r. Funktionen:

Eine rationale Funktion der Form (1) *ist dann und nur dann eine p. r. Funktion, wenn sie*

A. in der offenen rechten Halbebene analytisch ist und auf der imaginären Achse einschließlich des unendlich fernen Punktes höchstens einfache Pole hat;

B. die Residuen in diesen Polen positiv sind; und wenn

C. der Realteil von $f(z)$ für alle Punkte der imaginären Achse, in denen $f(z)$ regulär ist, nicht negativ wird.

2. Die Pilotybedingungen für p. r. Funktionen:

Eine rationale Funktion $f(z)$ der Form (1) *mit teilerfremdem Zähler und Nenner ist dann und nur dann eine p. r. Funktion, wenn*

A. $$C(z) + A(z) = H(z)$$

ein Hurwitzpolynom ist und wenn

B. $$C(it)\,A(-it) + C(-it)\,A(it) \geqq 0$$

ist für alle reellen t mit $-\infty < t < +\infty$.

Ein wichtiges Anwendungsgebiet der p. r. Funktionen ist die elektrische Netzwerktheorie. Nach O. Brune [2] können nämlich alle p. r. Funktionen und nur diese als Impedanzfunktionen von linearen Zweipolen (mit endlich vielen Schaltelementen) aufgefaßt werden. Für die Synthese von Zweipolen mit vorgeschriebenem Frequenzverhalten besitzt daher die Aufgabe, die p. r. Funktionen durch explizite Koeffizientenbedingungen zu charakterisieren und damit die erheblichen Rechenaufwand erfordernden rekursiven Verfahren zu vermeiden, praktische Bedeutung.

Gelöst ist diese Aufgabe bisher nur für einige Unterklassen von p. r. Funktionen [4], [5], [6], [7], [8], [9].

H. König [10] hat die explizite Charakterisierung der ganzen Klasse der p. r. Funktionen durch algebraische Gleichungen bzw. Ungleichungen zwischen den Koeffizienten von $f(z)$ untersucht und ist dabei zu dem Ergebnis gelangt, daß eine Charakterisierung durch das gleichzeitige Bestehen von endlich vielen Bedingungen dieser Art nicht möglich ist.

Aus diesem Ergebnis von H. König folgt zum Beispiel, daß die von J. Schur [11] angegebenen Kriterien für die Koeffizienten unimodular beschränkter Potenzreihen bei einer Übertragung auf p. r. Funktionen im allgemeinen Fall zu unendlich vielen Bedingungen führen müssen und daher nicht zur praktischen Nachprüfung der Zugehörigkeit einer vorgegebenen rationalen Funktion zur Klasse der p. r. Funktionen benutzt werden können.

In einer bedeutenden Arbeit hat Nai-Ta Ming [12] die in den Spulen und Kondensatoren von Zweipolen stets auftretenden Verluste dadurch berücksichtigt, daß er in Reihe mit jeder Spule und parallel zu jedem Kondensator einen Ohmschen Widerstand annimmt. Solche der physikalischen Wirklichkeit entsprechende Zweipole hat Nai-Ta Ming im Unterschied zu den idealisierten Zweipolen „Verlustzweipole" genannt. Ihre Impedanzfunktionen, die auch als „Verlustfunktionen" bezeichnet werden, besitzen die Eigenschaft, daß für ein $\varepsilon > 0$ mit $f(z)$ auch $f(z-\varepsilon)$ noch eine p. r. Funktion ist.

In der vorliegenden Arbeit wird eine explizite Lösung des Koeffizientenproblems der Verlustfunktionen angegeben.

I. Die Mingschen Bedingungen für Verlustfunktionen. Nach Nai-Ta Ming [12] ist eine beliebig vorgegebene rationale Funktion $f(z)$ dann und nur dann eine Verlustfunktion, wenn sie

a) für reelle z reell ist,

b) in der abgeschlossenen rechten Halbebene $\operatorname{Re} z \geqq 0$ regulär ist gegebenenfalls mit Ausnahme des unendlich fernen Punktes, wo ein einfacher Pol mit positiv reellem Residuum erlaubt ist, und wenn

c) der Realteil von $f(z)$ auf der imaginären Achse überall größer als Null ist, es sei denn, daß im Unendlichen eine einfache Nullstelle liegt; im letzteren Fall muß $\operatorname{Re} 1/f(z)$ für $z \to \infty$ einen positiven Grenzwert besitzen.

Setzt man $f(z)$ nun aber in der Form (1) mit teilerfremdem $C(z)$ und $A(z)$ und positivem c_0 und a_0[1]) voraus und berücksichtigt noch, daß das Polynom

$$P(t^2) \doteq A(it)\,C(-it) + A(-it)\,C(it)$$

bis auf einen positiven Faktor den Realteil von $f(z)$ auf der imaginären *it*-Achse darstellt, so können die oben angegebenen Bedingungen von Ming ersetzt werden durch:

Hilfssatz 1. *Eine rationale Funktion $f(z)$ von der Form* (1) *mit teilerfremdem $C(z)$ und $A(z)$ und positivem c_0 und a_0 ist dann und nur dann eine Verlustfunktion, wenn*

A. der Grad des Zählers sich höchstens um eins vom Grad des Nenners unterscheidet, wobei im Falle $m \neq n$ außerdem noch die Determinante

$$\begin{vmatrix} a_0 & a_1 \\ c_0 & c_1 \end{vmatrix}$$

für $m = n + 1$ positiv und für $m = n - 1$ negativ sein muß,

B. der Nenner $A(z)$ ein Hurwitzpolynom ist und wenn

C. $A(it)\,C(-it) + A(-it)\,C(it) > 0$ ist für alle reellen t mit $-\infty < t < +\infty$.

Da explizite Koeffizientenbedingungen für Hurwitzpolynome bekannt sind [13], besteht unsere Aufgabe also nur noch darin, derartige Bedingungen für positiv definite gerade Polynome aufzustellen.

II. Kennzeichnende Determinantenbedingungen für positiv definite gerade Polynome. Wir gehen aus von dem folgenden Satz, welcher in der Algebra [14] bewiesen wird:

Satz 1. *Die Anzahl der voneinander verschiedenen Wurzeln der Gleichung*

$$P(x) = d_0 x^n + d_1 x^{n-1} + \cdots + d_n = 0 \qquad (d_i \text{ reell}, d_0 > 0, n > 0)$$

ist gleich dem Rang, die Anzahl der verschiedenen reellen Wurzeln ist gleich der Signatur der quadratischen Form

$$F(x_1, x_2, \ldots, x_n) = \sum_{l=1}^{n} \sum_{m=1}^{n} s_{l+m-2}\, x_l\, x_m . \tag{2}$$

Hierbei bedeuten die s_j die Potenzsummen der Wurzeln β_i von $P(x) = 0$:

$$s_j(\beta_1, \beta_2, \ldots, \beta_n) = \beta_1^j + \beta_2^j + \cdots + \beta_n^j \qquad (j = 0, 1, 2, \ldots).$$

Denken wir uns diese Potenzsummen für ein gerades Polynom

$$P(t^2) = k_0 t^{2p} + k_1 t^{2p-2} + \cdots + k_p \qquad (k_i \text{ reell}, k_0 > 0, p > 0) \tag{3}$$

gebildet, so zeigt es sich, daß alle s_j mit ungeradem Index verschwinden, da mit β_i stets auch $-\beta_i$ eine Nullstelle (gleicher Ordnung) von $P(t^2)$ ist.

Die quadratische Form (2) läßt sich daher in einen geraden und einen ungeraden Teil zerlegen:

---

[1]) Diese Voraussetzung darf gemacht werden, da bei einer p. r. Funktion mit teilerfremdem Zähler und Nenner alle nicht verschwindenden Koeffizienten das gleiche Vorzeichen haben, was unmittelbar aus der Faktorzerlegung von Zähler und Nenner folgt.

$$F(x_1, x_2, \ldots, x_{2p}) = \sum_{l=1}^{2p} \sum_{m=1}^{2p} s_{l+m-2} x_l x_m = F_1(x_1, x_3, \ldots, x_{2p-1}) + F_2(x_2, x_4, \ldots, x_{2p})$$

mit

$$F_1(x_1, \ldots, x_{2p-1}) = \sum_{\varkappa=0}^{p-1} \sum_{\lambda=0}^{p-1} s_{2(\varkappa+\lambda)} x_{2\varkappa+1} x_{2\lambda+1}$$

und

$$F_2(x_2, \ldots, x_{2p}) = \sum_{\mu=1}^{p} \sum_{\nu=1}^{p} s_{2(\mu+\nu)-2} x_{2\mu} x_{2\nu}.$$

Unmittelbar aus der Definition der Signatur einer quadratischen Form folgt, daß die Signatur S von $F(x_1, x_2, \ldots, x_{2p})$, auf deren Bestimmung es ja ankommt, da $S = 0$ nach Satz 1 kennzeichnend für definite Polynome ist, gleich der Summe der Signaturen S_1 und S_2 der Formen $F_1(x_1, \ldots, x_{2p-1})$ und $F_2(x_2, \ldots, x_{2p})$ ist.

Bei F_1 und F_2 handelt es sich nun aber (ebenso wie bei F) um sogenannte „rekurrierende“ Formen, das heißt Formen, bei denen die Koeffizienten nur von der Summe der Indizes abhängen, und für die Signatur einer solchen Form gilt nach FROBENIUS [15]:

Satz 2. „*Zur Berechnung der Signatur einer beliebigen rekurrierenden Form . . .*

$$\left(F = \sum_{\alpha,\beta=0}^{n-1} a_{\alpha+\beta} x_\alpha x_\beta\right)$$

. . . ergibt sich . . . die folgende Regel: Unter den Determinanten . . .

(4) $$\left(A_0 = 1, A_1 = a_{11}, A_2 = \begin{vmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{vmatrix}, \ldots, A_r = \begin{vmatrix} a_{11} & \cdot & \cdot & \cdot & a_{1r} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{1r} & \cdot & \cdot & \cdot & a_{rr} \end{vmatrix}, \ r \text{ Rang der F}\right.$$

. . . seien

$$A_0, A_\alpha, A_\beta, A_\gamma, \ldots, A_\varkappa, A_\lambda, \ldots, A_\nu, A_\varrho \qquad (0 < \alpha < \beta < \ldots < \varrho)$$

von Null verschieden. Ist $\varrho < r$, so füge man dazu noch die Determinante A'_r. Unter den Differenzen der Indizes $\alpha, \beta - \alpha, \gamma - \beta, \ldots, r - \varrho$ behalte man nur die bei, welche ungerade sind. Ist $\lambda - \varkappa$ ungerade, so berechne man das Vorzeichen

$$(-1)^{\frac{1}{2}(\lambda-\varkappa-1)} \operatorname{sign}(A_\varkappa A_\lambda),$$

ist $r - \varrho$ ungerade, das Vorzeichen

$$(-1)^{\frac{1}{2}(r-\varrho-1)} \operatorname{sign}(A_\varrho A'_r).$$

Dann ist die Signatur der Form . . . gleich der Summe dieser Vorzeichen

$$s = \sum (-1)^{\frac{1}{2}(\lambda-\varkappa-1)} \operatorname{sign}(A_\varkappa A_\lambda) \ldots \qquad (\lambda - \varkappa \text{ ungerade}).“$$

In dieser Form ist die Regel von FROBENIUS für unseren Zweck noch ungeeignet, sie läßt sich aber in dem von uns behandelten Sonderfall auf eine brauchbare Form bringen, da, wie wir im folgenden beweisen werden, sowohl für F_1 als auch für F_2

1. die Determinanten A_i durch bestimmte andere Determinanten ersetzt werden können, in denen statt der zu $P(t^2)$ gehörigen Potenzsummen die Koeffizienten von $P(t^2)$ selbst vorkommen, und

2. die Determinante A_r nicht verschwindet, so daß auf den Fall $\varrho < r$ und damit also auf die (von FROBENIUS an anderer Stelle angegebene) Determinante A'_r überhaupt nicht eingegangen zu werden braucht.

Zu 1.: A. HURWITZ [13] beweist in seiner bekannten Arbeit über die Bedingungen, unter welchen eine Gleichung nur Wurzeln mit negativem Realteil besitzt, den Satz:

Satz 3. *Ist eine rationale Funktion in der Form*

$$R(z) = \frac{b_0 z^k + b_1 z^{k-1} + \cdots + b_k}{a_0 z^k + a_1 z^{k-1} + \cdots + a_k} \tag{5}$$

gegeben, wobei der Koeffizient a_0 von Null verschieden vorausgesetzt wird, und hat diese in der Umgebung von $z = \infty$ die Laurententwicklung

$$R(z) = c + \frac{c_0}{z} + \frac{c_1}{z^2} + \cdots,$$

so gilt für die Determinante

$$D_m = \begin{vmatrix} c_0 & c_1 & \cdot & \cdot & \cdot & c_{m-1} \\ c_1 & c_2 & \cdot & \cdot & \cdot & c_m \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ c_{m-1} & c_m & \cdot & \cdot & \cdot & c_{2m-2} \end{vmatrix}$$

die Beziehung

$$D_m = a_0^{-2m} \begin{vmatrix} a_0 & a_1 & \cdot & \cdot & \cdot & a_{2m-1} \\ b_0 & b_1 & \cdot & \cdot & \cdot & b_{2m-1} \\ 0 & a_0 & \cdot & \cdot & \cdot & a_{2m-2} \\ 0 & b_0 & \cdot & \cdot & \cdot & b_{2m-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & a_m \\ 0 & \cdot & \cdot & \cdot & \cdot & b_m \end{vmatrix} \quad (a_i, b_i = 0 \text{ für } i > k).$$

Wendet man diesen Satz auf die beiden rationalen Funktionen

$$R_1(z) = \left[\frac{1}{t} \cdot \frac{d\,P(t^2)/dt}{P(t^2)}\right]_{t^2=z} = \frac{2p\,k_0 z^{p-1} + (2p-2)\,k_1 z^{p-2} + \cdots + 2k_{p-1}}{k_0 z^p + k_1 z^{p-1} + \cdots + k_p}$$

und

$$R_2(z) = \left[t \cdot \frac{d\,P(t^2)/dt}{P(t^2)}\right]_{t^2=z} = \frac{2p\,k_0 z^p + (2p-2)\,k_1 z^{p-1} + \cdots + 2k_{p-1} z}{k_0 z^p + k_1 z^{p-1} + \cdots + k_p}$$

an, für welche in einer bestimmten Umgebung des Punktes $z = \infty$ die Laurententwicklungen

$$R_1(z) = \frac{s_0}{z} + \frac{s_2}{z^2} + \cdots + \frac{s_{2j}}{z^{j+1}} + \cdots$$

und

$$R_2(z) = s_0 + \frac{s_2}{z} + \cdots + \frac{s_{2j}}{z^j} + \cdots$$

($s_{2j}, \ldots$ zu $P(t^2)$ gehörige Potenzsummen) gelten, da bekanntlich für genügend große $|t|$

$$\frac{d\,P(t^2)/dt}{P(t^2)} = \frac{s_0}{t} + \frac{s_2}{t^3} + \cdots + \frac{s_{2j}}{t^{2j+1}} + \cdots$$

ist [16], so erhält man:

$$D'_m = \begin{vmatrix} s_0 & \cdot & \cdot & \cdot & s_{2m-2} \\ s_2 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ s_{2m-2} & \cdot & \cdot & \cdot & s_{4m-4} \end{vmatrix} = k_0^{-2m} \cdot 2^m \begin{vmatrix} k_0 & k_1 & \cdot & \cdot & \cdot & \cdot & \cdot & k_{2m-1} \\ 0 & p k_0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & k_0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & k_m \\ \cdot & \cdot & \cdot & \cdot & \cdot & & & (p-m+1)\,k_{m-1} \end{vmatrix}$$

und

$$D''_m = \begin{vmatrix} s_2 & \cdot & \cdot & \cdot & s_{2m} \\ s_4 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ s_{2m} & \cdot & \cdot & \cdot & s_{4m-2} \end{vmatrix} = k_0^{-2m} \cdot 2^m \begin{vmatrix} k_0 & k_1 & \cdot & \cdot & \cdot & k_{2m-1} \\ p k_0 & (p-1)\,k_1 & \cdot & \cdot & \cdot & \cdot \\ 0 & k_0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & k_m \\ \cdot & \cdot & \cdot & \cdot & \cdot & (p-m)\,k_m \end{vmatrix}$$

($k_i = 0$ für $i > p$).

In der Regel von Frobenius können damit also die Determinanten (4) durch die obigen explizit von den k_i abhängigen Determinanten ersetzt werden.

Zu 2.:

Hilfssatz 2. *Ist r der Rang der quadratischen Form F_1 bzw. F_2, so ist die Hauptunterdeterminante r-ten Grades der zur Form gehörigen Matrix von Null verschieden.*

Wir beweisen statt Hilfssatz 2 den allgemeineren

Hilfssatz 2a. *Enthalten der Zähler und der Nenner der rationalen Funktion* (5) *einen größten gemeinsamen Teiler q-ten ($q \geqq 0$) Grades, so hat die Matrix*

$$\mathfrak{M} = \begin{pmatrix} c_0 & c_1 & \cdot & \cdot & \cdot & c_{k-1} \\ c_1 & c_2 & \cdot & \cdot & \cdot & c_k \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ c_{k-1} & & \cdot & \cdot & \cdot & c_{2k-2} \end{pmatrix}$$

den Rang $r = k - q$, und ihre Hauptunterdeterminante r-ten Grades ist von Null verschieden.

Beweis. Zum Beweise denken wir uns bei der rationalen Funktion (5) den eventuell vorhandenen größten gemeinsamen Teiler von Zähler und Nenner weggekürzt und erhalten:

$$R(z) = P_1(z)/P_2(z)$$

mit

$$P_1(z) = B_0 z^r + B_1 z^{r-1} + \cdots + B_r$$

und

$$P_2(z) = A_0 z^r + A_1 z^{r-1} + \cdots + A_r$$

$$(A_0 \neq 0,\ r \leqq k).$$

Man sieht sofort, daß

$$D_r = \begin{vmatrix} c_0 & c_1 & \cdot & \cdot & \cdot & c_{r-1} \\ c_1 & c_2 & \cdot & \cdot & \cdot & c_r \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ c_{r-1} & & \cdot & \cdot & \cdot & c_{2r-2} \end{vmatrix}$$

verschieden von Null ist, denn diese Determinante stimmt nach Satz 3 bis auf einen von Null verschiedenen Faktor mit der Resultante von $P_1(z)$ und $P_2(z)$ überein, welche bekanntlich [17] bei zwei teilerfremden Polynomen nicht verschwindet.

Es braucht also nur noch gezeigt zu werden, daß der Rang der Matrix $\mathfrak{M}$ nicht größer als r ist. Wir multiplizieren zu diesem Zweck beide Seiten der Entwicklung

$$R(z) = c + \frac{c_0}{z} + \cdots + \frac{c_j}{z^{j+1}} + \cdots$$

mit $P_2(z)$ und erhalten:

$$P_1(z) = P^+(z) + \frac{\sum\limits_{i=0}^{r} A_i c_{r-i}}{z} + \cdots + \frac{\sum\limits_{i=0}^{r} A_i c_{j+r-i}}{z^{j+1}} + \cdots;$$

hierbei ist $P^+(z)$ ein Polynom, welches wegen der Eindeutigkeit einer solchen Entwicklung identisch mit $P_1(z)$ sein muß. Aus demselben Grunde verschwinden auch alle Koeffizienten

$$\sum_{i=0}^{r} A_i c_{j+r-i} \qquad (j = 0, 1, 2, \ldots).$$

Da A_0 von Null verschieden ist, kann man schreiben:

$$c_{r+j} = -\frac{A_1}{A_0} c_{r+j-1} - \frac{A_2}{A_0} c_{r+j-2} - \cdots - \frac{A_r}{A_0} c_j \qquad (j = 0, 1, 2, \ldots).$$

Wir erhalten also für die c_{r+j} eine lineare Rekursionsformel, so daß die Matrix $\mathfrak{M}$ durch geeignete Linearkombinationen von Zeilen bzw. Spalten auf die Form

$$\mathfrak{M}^* = \begin{pmatrix} c_0 & c_1 & \cdot & \cdot & \cdot & c_{r-1} & 0 & \cdot & \cdot & \cdot & 0 \\ c_1 & c_2 & \cdot & \cdot & \cdot & c_r & 0 & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ c_{r-1} & c_r & \cdot & \cdot & \cdot & c_{2r-2} & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \end{pmatrix}$$

gebracht werden kann; da diese Operation den Rang nicht verändert, folgt rg $\mathfrak{M} \leqq r$, womit der Hilfssatz 2a bewiesen ist.

Die Ergebnisse dieses Abschnitts können zu dem folgenden Determinantenkriterium für positiv definite Polynome zusammengefaßt werden:

Satz 4. *Ein gerades Polynom*

$$P(t^2) = k_0 t^{2p} + k_1 t^{2p-2} + \cdots + k_p \qquad (k_i \textit{ reell}, k_0 > 0, p > 0)$$

ist dann und nur dann für alle reellen Werte der Veränderlichen t positiv, wenn in den beiden aus den Hauptunterdeterminanten T_j der Matrix

$$\mathfrak{R} = \begin{pmatrix} pk_0 & (p-1)k_1 & (p-2)k_2 & \cdots & k_{p-1} & 0 & \cdots & \cdots & 0 \\ k_0 & k_1 & k_2 & \cdots & k_{p-1} & k_p & 0 & \cdots & 0 \\ 0 & pk_0 & (p-1)k_1 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdot \\ 0 & k_0 & k_1 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdot \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdot \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdot \\ \cdots & \cdots & \cdots & \cdots & 0 & pk_0 & \cdots & k_{p-1} & 0 \\ \cdots & \cdots & \cdots & \cdots & 0 & k_0 & \cdots & \cdots & k_p \end{pmatrix}$$

gebildeten Determinantenketten

(6a) $$1, T_1, T_3, \ldots, T_{2p-1}\ ^{2)}$$

und

(6b) $$1, T_2, T_4, \ldots, T_{2p}$$

die Differenz zwischen der Anzahl der Vorzeichenfolgen und der Anzahl der Vorzeichenwechsel gleich groß ist. Hierbei gilt für die Abzählung der Vorzeichenfolgen bzw. -wechsel die Regel:

a) Sind in der Kette (6a) *oder* (6b) *von einem bestimmten T_j an alle weiteren Determinanten Null, so brauchen diese bei der Abzählung nicht berücksichtigt zu werden.*

b) Verschwindet zwischen zwei von Null verschiedenen Determinanten $T_\varkappa$ und T_λ der Kette (6a) *bzw.* (6b) *eine ungerade Anzahl von Determinanten, so hat man den Zeichenwechsel oder die Zeichenfolge zwischen $T_\varkappa$ und T_λ nicht mitzuzählen.*

Verschwindet zwischen zwei von Null verschiedenen Determinanten $T_\varkappa$ und T_λ eine gerade Anzahl von Determinanten, so hat man,

falls es $4m$ $(m = 0, 1, 2, \ldots)$ *sind, eine Zeichenfolge zwischen $T_\varkappa$ und T_λ als Folge und einen Zeichenwechsel als Wechsel zu zählen,*

falls es $4m + 2$ $(m = 0, 1, 2, \ldots)$ *sind, eine Zeichenfolge zwischen $T_\varkappa$ und T_λ als Wechsel und einen Zeichenwechsel zwischen $T_\varkappa$ und T_λ als Folge zu zählen.*

III. Koeffizientenbedingungen für Verlustfunktionen. Aus Hilfssatz 1 und Satz 4 ergeben sich unter Berücksichtigung des bekannten Hurwitzkriteriums [13] die folgenden expliziten Koeffizientenbedingungen für Verlustfunktionen:

Satz 5. *Eine rationale Funktion $f(z)$ von der Form* (1) *mit teilerfremdem $C(z)$ und $A(z)$ und positivem c_0 und a_0 ist dann und nur dann eine Verlustfunktion, wenn*

A. der Grad des Zählers sich höchstens um eins vom Grad des Nenners unterscheidet, wobei im Falle $m \neq n$ außerdem noch die Determinante

$$\begin{vmatrix} a_0 & a_1 \\ c_0 & c_1 \end{vmatrix}$$

für $m = n + 1$ positiv und für $m = n - 1$ negativ sein muß,

2) Es ist sgn $T_{2j-1} = \operatorname{sgn} D'_j$ und sgn $T_{4i} = \operatorname{sgn} D''_{2i}$, aber sgn $T_{4i+2} \neq \operatorname{sgn} D''_{2i+1}$. Die Differenz zwischen den Vorzeichenfolgen und den Wechseln ist daher in (6a) gleich S_1, in (6b) jedoch gleich $-S_2$.

B. die Determinanten

$$\Delta_1 = a_1, \quad \Delta_2 = \begin{vmatrix} a_1 & a_3 \\ a_0 & a_2 \end{vmatrix}, \ldots, \Delta_\lambda = \begin{vmatrix} a_1 & a_3 & . & . & . & a_{2\lambda-1} \\ a_0 & a_2 & . & . & . & a_{2\lambda-2} \\ 0 & a_1 & . & . & . & . \\ & . & . & . & . & . \\ & . & . & . & . & a_\lambda \end{vmatrix}, \ldots, \Delta_n$$

$(a_i = 0$ *für* $i > n)$

sämtlich positiv sind und wenn (für $\mathrm{Min}(m, n) \geqq 1$*)*

C. das Polynom $A(it)\,C(-it) + A(-it)\,C(it)$ *die im Satz 4 angegebenen Determinantenbedingungen für positiv definite (gerade) Polynome erfüllt.*

IV. Bedingungen für eine allgemeinere Klasse von p. r. Funktionen. Die im vorigen Abschnitt aufgestellten Bedingungen für Verlustfunktionen lassen sich auch noch in dem allgemeineren Falle anwenden, daß die Funktion $f(z)$, welche in der Form (1) mit teilerfremdem Zähler und Nenner vorgegeben sei, gleich der Summe aus einer Verlust- und einer Reaktanzfunktion[3]) ist.

Mit Hilfe eines Satzes von H. Cremer und F. H. Effertz [18] kann nämlich zunächst entschieden werden, ob der Nenner $A(z)$ von $f(z)$ sich in der Form

$$A(z) = A_1(z)\,A_2(z)$$

zerlegen läßt, wobei $A_1(z)$ ein Hurwitzpolynom und $A_2(z)$ ein Polynom bedeutet, das nur symmetrisch zum Nullpunkt liegende Nullstellen hat.

Derselbe Satz gibt auch eine explizite Darstellung des Polynoms $A_2(z)$, so daß $f(z)$ als Summe aus einer für $\mathrm{Re}\, z \geqq 0$ (einschließlich $z = \infty$) regulären rationalen Funktion $f_1(z)$ und einer rationalen Funktion $f_2(z)$ geschrieben werden kann, deren Pole sämtlich symmetrisch zum Nullpunkt liegen. Die unbekannten Koeffizienten dieser Zerlegung ergeben sich dabei durch Koeffizientenvergleich als (eindeutige) Lösungen linearer Gleichungssysteme.

Die Funktion $f_2(z)$ muß nun aber, wie z. B. aus den Brunebedingungen für p. r. Funktionen folgt, eine Reaktanzfunktion[4]) sein, was mit Hilfe eines Determinantenkriteriums von W. Cauer [4] stets nachgeprüft werden kann, während $f_1(z)$ die Bedingungen des Satzes 5 für Verlustfunktionen erfüllen muß, wenn $f(z)$ zu der von uns betrachteten Klasse von p. r. Funktionen gehört.

Abschließend sei noch bemerkt, daß sich mit Hilfe der Untersuchungen des Abschnitts II sowie einer im Anschluß an den oben erwähnten Satz von H. Cremer und F. H. Effertz naheliegenden expliziten Darstellung des größten gemeinsamen Teilers eines (geraden) Polynoms und seiner ersten Ableitung ein allgemeines Determinantenverfahren für beliebige p. r. Funktionen angeben läßt, welches in einer Prüfung der in der Einleitung angegebenen Pilotybedingungen für p. r. Funktionen be-

---

[3]) d. i. eine p. r. Funktion, deren Realteil auf der imaginären Achse verschwindet.

[4]) Damit $f_2(z)$ sich nicht als Summe aus einer Reaktanzfunktion und einer Konstanten ergibt, muß (unter Berücksichtigung des oben erwähnten Kriteriums von Cauer) der Zähler von $f_2(z)$ als gerades oder ungerades Polynom angesetzt werden je nachdem, ob der Nenner $A_2(z)$ ungerade oder gerade ist.

steht. Wir gehen auf dieses Verfahren hier nicht näher ein, da wir es an anderer Stelle [19] bereits ausführlich dargestellt haben. Dort wird auch über Anwendungen der hier mitgeteilten Sätze in der Elektrotechnik berichtet, die Berührungspunkte mit einer kürzlich erschienenen Arbeit von A. H. Zemanian [20] aufweisen.

Literaturverzeichnis

[1] E. A. Guillemin, Synthesis of Passive Networks. New York 1957, p. 15.
[2] O. Brune, Synthesis of a Finite Two-Terminal Network whose Driving-Point Impedance is a Prescribed Function of Frequency. J. Math. Physics **10**, 191–236 (1931).
[3] H. Piloty, Über die Realisierbarkeitssätze der Kettenmatrix von Reaktanzvierpolen. Telegraphen-, Fernsprech-, Funk- und Fernseh-Technik **30**, 217–223 (1941).
[4] W. Cauer, Theorie der linearen Wechselstromschaltungen. 2. Auflage, Berlin 1954, p. 182.
[5] F. H. Effertz, On the Synthesis of Networks Containing two Kinds of Elements. Proc. Symp. Mod. Netw. Synthesis **5**, 145–173 (1955).
[6] K. H. Breuer und F. H. Effertz, Ein Algorithmus und ein Klassifikationsprinzip für Funktionen mit nichtnegativem Realteil. Math. Ann. **138**, 335–341 (1959).
[7] F. H. Effertz, Ein Rechenverfahren für die Stabilitätsbedingungen. Regelungstechnik, p. 368; Verlag Oldenbourg, München 1957.
[8] F. H. Effertz, On the relation between the stability boundary surfaces of linear and nonlinear servomechanisms and the realizability boundary surfaces of some classes of frequency characteristics of electrical networks, in W. Cauer, Synthesis of linear communication networks, vol. II. p. 840–856, Verlag McGraw Hill, New York 1958.
[9] F. H. Effertz, Beschränkte Funktionen, Frequenzcharakteristiken elektrischer Netzwerke und algebraische Stabilitätskriterien. Z. angew. Math. Mech. **33**, 281–283 (1953).
[10] H. König, Zur Charakterisierung der positiven rationalen Funktionen. Arch. Math. **8**, 409–412 (1957).
[11] J. Schur, Über Potenzreihen, die im Innern des Einheitskreises beschränkt sind, I. J. reine angew. Math. **147**, 205–232 (1917).
[12] Nai-Ta Ming, Verwirklichung von linearen Zweipolschaltungen vorgeschriebener Frequenzabhängigkeit unter Berücksichtigung der Verluste von Spulen und Kondensatoren. Arch. Elektrotechnik **39**, 359–387 (1949).
[13] A. Hurwitz, Über die Bedingungen, unter welchen eine Gleichung nur Wurzeln mit negativen reellen Teilen besitzt. Math. Ann. **46**, 273–284 (1895).
[14] O. Perron, Algebra II. Göschens Lehrbücherei, Bd. 9, Berlin 1951, p. 2.
[15] G. Frobenius, Über das Trägheitsgesetz der quadratischen Formen. S.-Ber. königl. preuß. Akad.Wiss Berlin XII (1894), p. 241, XXIII (1894), p. 407.
[16] H. Weber, Kleines Lehrbuch der Algebra. Verlag von F. Vieweg & S., Braunschweig 1912, p. 62.
[17] O. Perron, Algebra I. Göschens Lehrbücherei, Bd. 8, Berlin 1951, p. 206
[18] H. Cremer und F. H. Effertz, Über die algebraischen Kriterien für die Stabilität von Regelungssystemen. Math. Ann. **137**, 328–350 (1959).
[19] F. H. Effertz und W. Meuffels, Über Realisierbarkeitsbedingungen für die Impedanzfunktionen zweipoliger elektrischer Netzwerke unter Berücksichtigung der Verluste von Spulen und Kondensatoren. Arch. Elektrotechnik **45**, 418–428 (1960).
[20] A. H. Zemanian, Generalizations of the Concept of Positive Real Functions. IRE Transactions on Circuit Theory **6**, 374–382 (1959).

Eingegangen am 1. 8. 1960

Anschrift der Autoren:

F. H. Effertz
Krefeld
Goethestraße 108

W. Meuffels
Wassenberg
Erkelenzer Straße 106

Distributivität und subdirekte Zerlegbarkeit vollständiger Verbände

Von

Günter Bruns

1. In dieser Note sei L stets ein vollständiger Verband und $\mathfrak{M}$ ein alle einelementigen Teilmengen von L enthaltendes, sonst aber zunächst beliebiges System von Teilmengen von L. Wir betrachten das Distributivgesetz

$$(D_{\mathfrak{M}}) \qquad \bigwedge_{i\in I} \bigvee_{j\in J_i} x_{ij} = \bigvee_{\alpha\in\Pi J_i} \bigwedge_{i\in I} x_{i\alpha(i)},$$

wenn für alle $i \in I$ *stets* $\{x_{ij} | j \in J_i\} \in \mathfrak{M}$.

Dabei sei I ein beliebiger Indexbereich, jedem $i \in I$ zugeordnet ein weiterer beliebiger Indexbereich J_i und schließlich jedem (i, j) mit $j \in J_i$ zugeordnet ein Element $x_{ij} \in L$. Weiter sei ΠJ_i das über alle $i \in I$ zu erstreckende direkte Produkt der Mengen J_i, die Menge aller (eindeutigen) Abbildungen α also, deren Definitionsbereich I ist und die jedem $i \in I$ ein Element $\alpha(i) \in J_i$ zuordnen.

Wir benötigen ferner den Begriff der $\mathfrak{M}$-subdirekten Darstellung des Verbandes L[1]). Hierunter verstehen wir hier ein geordnetes Paar $(\{K_\beta\}_{\beta\in B}, \varphi)$, bestehend aus einer Familie $\{K_\beta\}_{\beta\in B}$ vollständiger Ketten (totalgeordneter Mengen) K_β und einem Ordnungsisomorphismus φ von L in das (geordnete) direkte Produkt $\prod_{\beta\in B} K_\beta$, der für jede Menge $M \in \mathfrak{M}$ der Bedingung $\varphi(\bigvee M) = \bigvee \varphi(M)$ und für jede beliebige Teilmenge T von L der Bedingung $\varphi(\bigwedge T) = \bigwedge \varphi(T)$ genügt.

G. N. Raney[2]) hat den Satz bewiesen, daß, wenn $\mathfrak{M}$ das System aller Teilmengen von L ist, das Distributivgesetz $(D_{\mathfrak{M}})$ mit der Existenz einer $\mathfrak{M}$-subdirekten Darstellung gleichbedeutend ist. Dieser Satz soll hier für eine größere Klasse von Systemen $\mathfrak{M}$ bewiesen werden. Systeme von der Art, wie wir sie hier zulassen werden, wurden in einem Spezialfall wohl zuerst von S. Papert[3]) betrachtet und zur Charakterisierung des Verbandes der abgeschlossenen Mengen eines topologischen Raumes durch Distributivitätseigenschaften herangezogen. Unser Satz enthält die Resultate von Raney und Papert als Spezialfälle, ist aber noch in allgemeineren Fällen gültig.

2. Wir definieren bei vorgegebenem $\mathfrak{M}$ weitere Systeme $\mathfrak{M}^+$ und $\mathfrak{M}^*$ wie folgt:

$M \in \mathfrak{M}^+$ *genau dann, wenn* $\{x_{ij} | i \in I, j \in J_i\}$ *so existiert, daß*

$$M = \{\bigwedge_{i\in I} x_{i\alpha(i)} | \alpha \in \Pi J_i\}$$

und bei festem $i \in I$ *stets* $\{x_{ij} | j \in J_i\} \in \mathfrak{M}$ *gilt;*

---

1) Zum allgemeinen Begriff des subdirekten Produktes siehe Birkhoff [1], S. 91ff.

2) Raney [3]. 3) S. Papert [2].

$M \in \mathfrak{M}^*$ genau dann, wenn $\{x_{ij} \mid i \in I, j \in J_i\}$ so existiert, daß

$$\{\bigvee_{j \in J_i} x_{ij} \mid i \in I\} \in \mathfrak{M}, \quad M = \{x_{ij} \mid i \in I, j \in J_i\}$$

und bei festem $i \in I$ stets $\{x_{ij} \mid j \in J_i\} \in \mathfrak{M}$ gilt.

Ein Mengensystem $\mathfrak{M}$ möge *distributiv abgeschlossen* heißen, wenn $\mathfrak{M}^+ \subseteq \mathfrak{M}$ und $\mathfrak{M}^* \subseteq \mathfrak{M}$ gilt.

Offenbar ist das System aller distributiv abgeschlossenen Systeme von Teilmengen von L ein Hüllensystem über der Potenzmenge $\mathfrak{P}L$ von L, so daß also insbesondere zu jedem System $\mathfrak{A} \subseteq \mathfrak{P}L$ ein kleinstes $\mathfrak{A}$ umfassendes, distributiv abgeschlossenes System, die distributiv abgeschlossene Hülle von $\mathfrak{A}$, existiert.

Neben der ursprünglichen Ordnung $\leqq$ von L spielt eine weitere binäre Relation $\lhd$ in L eine Rolle, die wir wie folgt definieren[4]:

$x \lhd y$ genau dann, wenn jede Menge $M \in \mathfrak{M}$, für die $\bigvee M \geqq y$ gilt, ein Element $z \in M$ mit $z \geqq x$ enthält.

Man bemerkt sofort die einfachen Regeln:

wenn $x \lhd y$, *so* $x \leqq y$,
wenn $x \leqq y$ *und* $y \lhd z$, *so* $x \lhd z$,
wenn $x \lhd y$ *und* $y \leqq z$, *so* $x \lhd z$.

3. Der Beweis unseres Satzes erfolgt nun mittels einiger Hilfssätze.

Hilfssatz 1[5]. *Ist $\mathfrak{M}^+ \subseteq \mathfrak{M}$ und genügt L dem Distributivgesetz $(D_{\mathfrak{M}})$, so existiert zu jedem $x \in L$ eine Menge $M_x \in \mathfrak{M}$ mit folgenden Eigenschaften:*

(1) $$x \leqq \bigvee M_x\,,$$

(2) *für alle $y \in L$ gilt: $y \lhd x$ genau dann, wenn ein Element $z \in M_x$ mit $y \leqq z$ existiert.*

Beweis. Das System aller Mengen $M \in \mathfrak{M}$, für die $\bigvee M \geqq x$ gilt, können wir in der Form $\{\{x_{ij} \mid j \in J_i\} \mid i \in I\}$ schreiben. Dann hat man wegen $(D_{\mathfrak{M}})$:

(3) $$x \leqq \bigwedge_{i \in I} \bigvee_{j \in J_i} x_{ij} = \bigvee_{\alpha \in \Pi J_i} \bigwedge_{i \in I} x_{i\alpha(i)}\,.$$

Man setze $M_x = \{\bigwedge_{i \in I} x_{i\alpha(i)} \mid \alpha \in \Pi J_i\}$. Wegen $\mathfrak{M}^+ \subseteq \mathfrak{M}$ gilt $M_x \in \mathfrak{M}$ und wegen (3): $\bigvee M_x \geqq x$. Ist aber $y \lhd x$, so enthält nach Definition jede der Mengen $\{x_{ij} \mid j \in J_i\}$ ein Element $x_{i\alpha(i)} \geqq y$, d. h. es existiert eine Abbildung $\alpha \in \Pi J_i$ mit $y \leqq \bigwedge_{i \in I} x_{i\alpha(i)} = z \in M_x$. Umgekehrt folgt aus der Konstruktion von M_x sofort, daß für jedes $z \in M_x$ stets $z \lhd x$ gilt, um so mehr also für jedes Element $y \leqq z$, womit Hilfssatz 1 bewiesen ist.

Hilfssatz 2[6]. *Genügt L dem Distributivgesetz $(D_{\mathfrak{M}})$ und ist $\mathfrak{M}$ distributiv abgeschlossen, so existiert zu je zwei der Bedingung $x \lhd y$ genügenden Elementen $x, y \in L$ ein Element $z \in L$ mit $x \lhd z \lhd y$.*

---

[4]) Diese Relation im Spezialfall auch bei PAPERT [2], S. 174, ferner implizit bei RANEY [3], S. 520.

[5]) Vgl. PAPERT [2], S. 175, Prop. 5.

[6]) Vgl. PAPERT [2], S. 175, Prop. 6.

Beweis. Wäre für jedes $z_i \in M_y$ stets $x \ntriangleleft z_i$, so existierte zu jedem $z_i \in M_y$ eine Menge $\{x_{ij} \mid j \in J_i\} \in \mathfrak{M}$ mit $\bigvee_{j \in J_i} x_{ij} \geqq z_i$ und $x_{ij} \ngeq x$. Wir setzen $x'_{ij} = x_{ij} \wedge z_i$. Da $\mathfrak{M}$ alle einelementigen Teilmengen von L enthält, folgte:

$$z_i = z_i \wedge \bigvee_{j \in J_i} x_{ij} = \bigvee_{j \in J_i} (z_i \wedge x_{ij}) = \bigvee_{j \in J_i} x'_{ij} \quad \text{und} \quad x'_{ij} \ngeq x .$$

Wegen $\mathfrak{M}^+ \subseteqq \mathfrak{M}$ gehören aber auch die Mengen $\{x'_{ij} \mid j \in J_i\}$ zu $\mathfrak{M}$, wegen $\mathfrak{M}^* \subseteqq \mathfrak{M}$ und $M_y = \{\bigvee_{j \in J_i} x'_{ij} \mid i \in I\}$ wäre also auch $\{x'_{ij} \mid i \in I,\, j \in J_i\} \in \mathfrak{M}$, aber $\bigvee_{\substack{i \in I \\ j \in J_i}} x'_{ij} \geqq y$ und $x'_{ij} \ngeq x$ für alle i, j, also auch $x \ntriangleleft y$, im Widerspruch zur Voraussetzung $x \lhd y$. Damit existiert also ein Element $z \in M_y$ mit $x \lhd z \lhd y$, w. z. b. w.

Wir wollen eine Teilmenge K' von L *zulässig* nennen, wenn zu jedem Element $k \in K'$ ein Element $k' \in K'$ (nicht notwendig $k \neq k'$) mit $k \lhd k'$ existiert. Dann gilt

Hilfssatz 3. *Genügt L dem Distributivgesetz $(D_{\mathfrak{M}})$ bei distributiv abgeschlossenem $\mathfrak{M}$, so existiert zu je zwei der Bedingung $x \nleqq y$ genügenden Elementen $x, y \in L$ eine vollständige Kette $K \subseteqq L$ mit folgenden Eigenschaften:*

(4) *Suprema beliebiger Teilmengen von K (in K gebildet) stimmen mit den entsprechenden in L gebildeten Suprema überein,*
(5) *zu jedem $k_0 \in K$ existiert eine zulässige Menge $K' \subseteqq K$ mit $\bigvee K' = k_0$,*
(6) *es existiert ein Element $k \in K$ mit $k \leqq x$ und $k \nleqq y$.*

Beweis. Ist $x \nleqq y$, so existiert nach Hilfssatz 1 ein Element $c \in L$ mit $c \lhd x$ und $c \nleqq y$. Sei K_0 eine x und c enthaltende Teilmenge von L, von der je zwei (verschiedene) Elemente k_1, k_2 entweder in der Relation $k_1 \lhd k_2$ oder in der Relation $k_2 \lhd k_1$ (insbesondere also auch in einer der Relationen $k_1 < k_2$ oder $k_2 < k_1$) stehen und die maximal bezüglich dieser Eigenschaft ist. (Auswahlaxiom!) Sei K die Menge der Suprema (bzgl. L gebildet) aller zulässigen Teilmengen von K_0. Wir behaupten: Die Menge K hat die im Hilfssatz geforderten Eigenschaften. Als Menge von oberen Grenzen von Teilmengen der totalgeordneten Menge K_0 ist auch K totalgeordnet. Ferner folgt aus der Definition von K sofort, daß das Supremum (in L gebildet) jeder beliebigen Teilmenge von K wieder zu K gehört, K also vollständig ist und der Bedingung (4) genügt. Zum Nachweis von (5) und (6) zeigen wir zunächst: Ist die Menge $K'_0 \subseteqq K_0$ zulässig und $k_0 = \bigvee K'_0$, so existiert zu jedem Element $k'_0 \in K'_0$ ein Element $k'' \in K$, das den Bedingungen $k'_0 \lhd k'' \lhd k_0$ genügt. Nach Definition der Zulässigkeit existieren nämlich zunächst Elemente $k''_0, k'''_0 \in K'_0$ mit $k'_0 \lhd k''_0 \lhd k'''_0 \leqq k_0$. Wegen der Maximalität von K_0 existiert nach Hilfssatz 2 (vollständige Induktion) eine Folge k'_1, $k'_2, \ldots, k'_n, \ldots$ von Elementen $k'_n \in K_0$ mit $k'_0 \lhd k'_1 \lhd k'_2 \lhd \cdots \lhd k'_n \lhd \cdots \leqq k''_0$. Da die Menge $\{k'_1, k'_2, \ldots, k'_n, \ldots\}$ zulässig ist, gehört $k'' = \bigvee_{n}^{1,\infty} k'_n$ zu K und man hat: $k'_0 \lhd$ $\lhd k'_1 \leqq k'' \leqq k''_0 \lhd k_0$, also $k'_0 \lhd k'' \lhd k_0$, wie behauptet. — Zum Beweis von (5) sei nun $k_0 \in K$ beliebig vorgegeben und sei $K' = \{k \mid k \in K \text{ und } k \lhd k_0\}$. Sei ferner K'_0 eine nach Definition existierende zulässige Teilmenge von K_0 mit $\bigvee K'_0 = k_0$. Dann existiert, wie wir gerade gesehen haben, zu jedem Element $k'_0 \in K'_0$ ein Element $k'' \in K'$ mit $k'_0 \leqq k''$, woraus bereits $\bigvee K' = k_0$ folgt. Zum Beweis der Zulässigkeit

von K' dürfen wir o. B. d. A. $k_0 \not\triangleleft k_0$ annehmen, denn andernfalls wäre $k_0 \in K'$ und also K' trivialerweise zulässig. Sei unter dieser Voraussetzung $k' \in K'$, also $k' < k_0$. Wegen $\bigvee K_0' = k_0$ existiert dann ein Element $k_0' \in K_0'$ mit $k' \leqq k_0'$, hierzu, wie wir oben gezeigt haben, ein Element $k'' \in K$ mit $k_0' \triangleleft k'' \triangleleft k_0$, womit also K' als zulässig erkannt und die Behauptung (5) bewiesen ist. — Zum Beweis von (6) schließlich existiert wegen $x, c \in K_0$, der Maximalität von K_0 und Hilfssatz 2 eine Folge k_1, $k_2, \ldots, k_n, \ldots$ von Elementen $k_n \in K_0$ mit $c \triangleleft k_1 \triangleleft k_2 \triangleleft \ldots \triangleleft k_n \triangleleft \ldots \leqq x$, deren Supremum $k = \bigvee_n^{1,\infty} k_n$ offensichtlich zu K gehört und die in (6) geforderte Eigenschaft hat. Damit ist auch Hilfssatz 3 bewiesen.

Hilfssatz 4. *Ist K eine beliebige den Bedingungen* (4) *und* (5) *genügende vollständige Kette aus L, und definiert man eine Abbildung φ_K von L durch $\varphi_K x = \bigvee \{k \mid k \leqq x$ und $k \in K\}$, so ist φ_K eine monotone Abbildung von L in (sogar auf) K, die für jede Menge $M \in \mathfrak{M}$ der Bedingung $\varphi_K(\bigvee M) = \bigvee \varphi_K(M)$ und für jede beliebige Teilmenge T von L der Bedingung*[7] $\varphi_K(\bigwedge T) = \bigwedge_K \varphi_K(T)$ *genügt.*

Beweis. Offensichtlich folgt aus $x \leqq y$ stets $\varphi_K x \leqq \varphi_K y$, woraus sich für beliebige Teilmengen M und T von L sofort

$$\bigvee \varphi_K(M) \leqq \varphi_K(\bigvee M) \tag{7}$$

und

$$\varphi_K(\bigwedge T) \leqq \bigwedge_K \varphi_K(T) \tag{8}$$

ergibt. Ist $M \in \mathfrak{M}$, so gilt aber auch:

$$\varphi_K(\bigvee M) \leqq \bigvee \varphi_K(M). \tag{9}$$

Zum Beweis sei $k_0 = \varphi_K(\bigvee M)$. Wegen (4) und nach Definition von φ_K ist dann insbesondere $k_0 \leqq \bigvee M$. Wegen (5) existiert eine zulässige Menge $K' \subseteq K$ mit $\bigvee K' = k_0$, für deren Elemente $k' \in K'$ dann also insbesondere $k' \triangleleft k_0$ gilt. Wegen $M \in \mathfrak{M}$ und $k_0 \leqq \bigvee M$ existiert also zu jedem $k' \in K'$ ein Element $x_{k'} \in M$ mit $k' \leqq x_{k'}$. Hieraus folgt aber: $k_0 = \bigvee K' \leqq \bigvee \{k \mid k \in K$ und $k \leqq x_{k'}$ für mindestens ein $k' \in K'\} \leqq \bigvee_{x \in M} \bigvee \{k \mid k \in K$ und $k \leqq x\} = \bigvee \varphi_K(M)$, die Behauptung (9). — Es bleibt noch

$$\bigwedge_K \varphi_K(T) \leqq \varphi_K(\bigwedge T) \tag{10}$$

zu zeigen. Für eine vollständige, totalgeordnete Menge K gilt das Distributivgesetz $(D_{\mathfrak{M}})$ sogar, wenn $\mathfrak{M}$ das System aller Teilmengen von K ist. Demnach hat man (k immer Elemente von K): $\bigwedge_K \varphi_K(T) = \bigwedge_{K, t \in T} \bigvee_{k \leqq t} k = \bigvee_{f \in F} \bigwedge_{t \in T} f(t)$, wobei F die Menge aller Abbildungen f ist, deren Definitionsbereich T ist, und die jedem Element $t \in T$ ein Element $f(t) \leqq t$, $f(t) \in K$ zuordnen. Damit gilt aber für alle $f \in F$:

---

[7]) Infima in L und K brauchen nicht übereinzustimmen. Wir hängen daher, wo Mißverständnisse zu befürchten sind, das Zeichen für den Verband, in dem die Infima (und entsprechend später Suprema) zu bilden sind, als Index an das Zeichen „$\bigwedge$" (bzw. „$\bigvee$") an.

$$\bigwedge_{t \in T}{}_K f(t) \leqq \bigwedge_{t \in T} f(t) \leqq \bigwedge T$$

und also

$$\bigvee_{f \in F} \bigwedge_{t \in T}{}_K f(t) \leqq \bigvee \{k \mid k \leqq \bigwedge T\} = \varphi_K(\bigwedge T),$$

w.z.b.w.

4. Aus unseren Hilfssätzen ergibt sich nun leicht als Hauptresultat der Note der angekündigte

Satz. *Ist $\mathfrak{M}$ distributiv abgeschlossen, so genügt der vollständige Verband L dem Distributivgesetz $(D_{\mathfrak{M}})$ genau dann, wenn er eine $\mathfrak{M}$-subdirekte Darstellung besitzt.*

Beweis. Wir zeigen zunächst, daß die Distributivität notwendig ist. Hierzu dürfen wir den Verband L unmittelbar als Teilmenge des Produktes $P = \prod_{\beta \in \mathsf{B}} K_\beta$ der vollständigen Ketten K_β auffassen, wobei die Suprema der Mengen $M \in \mathfrak{M}$ und beliebige Infima von Teilmengen von L in P und L übereinstimmen. Sei nun $\{x_{ij} \mid i \in I, j \in J_i\} \subseteq L$ und bei beliebigem $i \in I$ stets $\{x_{ij} \mid j \in J_i\} \in \mathfrak{M}$. Dann hat man, da das Distributivgesetz $(D_{\mathfrak{M}})$ in P sogar für das System aller Teilmengen von P gilt:

$$\bigwedge_{i \in I}{}_L \bigvee_{j \in J_i}{}_L x_{ij} = \bigwedge_{i \in I}{}_P \bigvee_{j \in J_i}{}_P x_{ij} = \bigvee_{\alpha \in \Pi J_i}{}_P \bigwedge_{i \in I}{}_P x_{i\alpha(i)} = \bigvee_{\alpha \in \Pi J_i}{}_P \bigwedge_{i \in I}{}_L x_{i\alpha(i)}.$$

Auf Grund dieser Gleichung liegt aber das Supremum $\bigvee_{\alpha \in \Pi J_i}{}_P \bigwedge_{i \in I}{}_L x_{i\alpha(i)}$ in L, d.h. es ist

$$\bigvee_{\alpha \in \Pi J_i}{}_P \bigwedge_{i \in I}{}_L x_{i\alpha(i)} = \bigvee_{\alpha \in \Pi J_i}{}_L \bigwedge_{i \in I}{}_L x_{i\alpha(i)},$$

womit die Distributivität bewiesen ist.

Sei jetzt umgekehrt das Distributivgesetz $(D_{\mathfrak{M}})$ erfüllt. Sei $\{K_\beta\}_{\beta \in \mathsf{B}}$ das System aller vollständigen Ketten K_β aus L, die den Bedingungen (4) und (5) genügen. Wir definieren eine Abbildung φ von L in das direkte Produkt $P = \prod_{\beta \in \mathsf{B}} K_\beta$ durch $pr_\beta(\varphi x) = \varphi_{K_\beta} x$ für alle $\beta \in \mathsf{B}$, durch die Vorschrift also, daß der Wert der Funktion φx (φx soll bei festem x ja eine Abbildung von B in die K_β sein) an der Stelle β, anders ausgedrückt: die β-te Projektion von φx, gleich dem in Hilfssatz 4 definierten Wert $\varphi_{K_\beta} x$ sein soll. Aus Hilfssatz 4 ergeben sich automatisch die Monotonie von φ und die Beziehungen $\varphi(\bigvee_L M) = \bigvee_P \varphi(M)$ $(M \in \mathfrak{M})$ und $\varphi(\bigwedge_L T) = \bigwedge_P \varphi(T)$ ($T \subseteq L$ beliebig). Es bleibt lediglich zu zeigen, daß φ ein Ordnungsisomorphismus ist, also aus $x \nleqq y$ in L stets $\varphi x \nleqq \varphi y$ folgt. Ist aber $x \nleqq y$, so existiert nach Hilfssatz 3 eine vollständige Kette K_β, die ein Element $k \leq x$, $k \nleqq y$ enthält. Dann ist aber $\varphi_{K_\beta} x > \varphi_{K_\beta} y$, d.h. $pr_\beta(\varphi x) \nleqq pr_\beta(\varphi y)$ und damit auch $\varphi x \nleqq \varphi y$, w.z.b.w.

Da das System aller Teilmengen von L offensichtlich distributiv abgeschlossen ist, ergibt sich der eingangs zitierte Satz von Raney als unmittelbarer Spezialfall unseres Satzes. Aber auch das zitierte Resultat von S. Papert läßt sich leicht folgern. Wir formulieren es als

Korollar. *Genau dann ist der vollständige Verband L dem System der abgeschlossenen Mengen eines topologischen Raumes isomorph, wenn er dem Distributivgesetz $(D_{\mathfrak{M}})$ genügt, wobei $\mathfrak{M}$ die distributiv abgeschlossene Hülle des Systems aller endlichen Teilmengen von L ist.*

Beweis. Der Nachweis der Notwendigkeit des Distributivgesetzes verläuft automatisch und soll hier nicht reproduziert werden. Ist aber umgekehrt das Distributivgesetz $(D_{\mathfrak{M}})$ erfüllt, so sei $(\{K_\beta\}_{\beta \in \mathsf{B}}, \varphi)$ eine der auf Grund unseres Satzes existierenden $\mathfrak{M}$-subdirekten Darstellungen von L. Wir definieren eine Abbildung ψ von L durch $\psi x = \{k \mid$ *Es existiert ein* $\beta \in \mathsf{B}$ *mit* $k \in K_\beta$ *und* $k \leqq pr_\beta(\varphi x)\}$. Sieht man das System aller Mengen ψx als durch die Beziehung der mengentheoretischen Inklusion geordnet an, so folgt leicht, daß ψ ein Ordnungsisomorphismus ist, der die Suprema endlicher Teilmengen von L in mengentheoretische Vereinigungen und die Infima beliebiger Teilmengen von L in mengentheoretische Durchschnitte überführt. Damit läßt sich $\psi(L)$ also als System aller abgeschlossenen Mengen eines topologischen Raumes auffassen, das L isomorph ist, w.z.b.w.

Literaturverzeichnis

[1] G. Birkhoff, Lattice theory. Amer. Math. Soc. Coll. Publ. **XXV**, New York 1948.

[2] S. Papert, Which distributive lattices are lattices of closed sets? Proc. Cambridge Philos. Soc. **55**, 172—176 (1959).

[3] G. N. Raney, A subdirect-union representation for completely distributive complete lattices. Proc. Amer. Math. Soc. **4**, 518—522 (1953).

Eingegangen am 8. 9. 1960

Anschrift des Autors:

Günter Bruns
Mathematisches Institut der Universität
Mainz, Saarstraße

A Note on F-Spaces

By

Leonard Gillman[1])

A completely regular space X is called an *F-space* when all finitely generated ideals in the ring $C(X)$ are principal ideals. Henriksen and I introduced the study of F-spaces in [1], obtaining a number of characterizations of these spaces. One of them is:

Theorem A. *X is an F-space if and only if for every $f \in C(X)$, the sets*

$$\operatorname{pos} f = \{x : f(x) > 0\} \quad \textit{and} \quad \operatorname{neg} f = \{x : f(x) < 0\}$$

are completely seperated

— i.e., $f = k|f|$ for some $k \in C(X)$. Extremally disconnected spaces [2, 1H] are always F-spaces. A less obvious example is the space $\beta\mathbf{R} - \mathbf{R}$. (As usual, βX denotes the Stone-Čech compactification of the space X.) That it is an F-space is a consequence of the following general theorem, also proved in [1]:

Theorem B. *If X is locally compact and σ-compact, then $\beta X - X$ is an F-space.*

A discussion of the main facts about F-spaces, including a new proof of B, is contained in [2, Chapter 14]. For general background, the reader is also referred to [2].

We have wondered from time to time whether Theorem B can be strengthened by weakening its hypothesis in a natural way: replacing "σ-compact" by "realcompact". The latter term may be defined as follows. Recall that a *zero-set* is the set of zeros of a continuous function, and that a *z-ultrafilter* is a maximal family of zero-sets with the finite intersection property; a *realcompact* space is then one on which every z-ultrafilter with the countable intersection property has nonempty intersection [2, Chapter 8]. The purpose of this note is to supply a counterexample: we construct a space X that is locally compact and realcompact but such that $\beta X - X$ is not an F-space.

By the way, neither of the conditions in B is necessary. To see this, it is enough to consider any uncountable, extremally disconnected space S in which no point has a compact neighborhood. (E.g., let S be an uncountable sum of replicas of the space defined in [3, 4.2].) Then S is *neither* locally compact nor σ-compact. Since S is extremally disconnected, so is βS. Since no point of S has a compact neighborhood in S, $\beta S - S$ is dense in βS. Therefore $\beta S - S$ is extremally disconnected, and so it is an F-space.

In what follows, I_r denotes the closed interval $[-r, r]$ (where $r > 0$), and D denotes

[1]) National Science Foundation Senior Post-Doctoral Fellow.

the discrete space of cardinal $\aleph_1$. Then D is realcompact [2, 8.18] and therefore so is the product

$$X = I_1 \times D$$

[2, 8.11]. Obviously, X is locally compact.

Let E denote the subspace

$$\{(0, \delta): \delta \in D\}$$

of X. The family of all subsets of E whose complements in E are countable has the finite intersection property; therefore there is a point p common to their closures in the compact space βX. It is evident that $p \in \beta X - X$ and that every neighborhood (in βX) of p meets E in an uncountable set.

Define

$$g(r, \delta) = r.$$

As a bounded continuous function on X, g has a continuous extension to all of βX; let f denote the restriction to $\beta X - X$ of this extension. We show that f changes sign in every neighborhood (in $\beta X - X$) of p — which proves that $\beta X - X$ is not an F-space.

Given any such neighborhood U, let V be a closed neighborhood of p in βX for which $V - X \subset U$. The interior (in βX) of V meets E in an uncountable set B. For each $\delta \in B$, V contains a set

$$I_{r_\delta} \times \{\delta\},$$

with r_δ rational. Hence B has an infinite (in fact, uncountable) subset A such that r_δ is constant — say $r_\delta = r$ — for all $\delta \in A$. The set

$$\{(r, \delta): \delta \in A\}$$

has a limit point p^+ in $V - X$. Obviously,

$$f(p^+) = g(r, \delta) = r > 0.$$

Similarly, U contains a point p^- such that $f(p^-) = -r < 0$.

References

[1] L. Gillman and M. Henriksen, Rings of continuous functions in which every finitely generated ideal is principal. Trans. Amer. Math. Soc. 82, 362—391 (1956).
[2] L. Gillman and M. Jerison, Rings of continuous functions. Princeton 1960.
[3] C. W. Kohls, Prime ideals in rings of continuous functions. Illinois J. Math. 2, 505—536 (1958).

Eingegangen am 8. 4. 1960

Anschrift des Autors:
Leonard Gillman
The University of Rochester
Rochester 20 (N.Y.), USA

Einige Bemerkungen über vollsymmetrische Banachsche Algebren

Von

James M. G. Fell und Elmar Thoma

Wir benützen die Terminologie und die Bezeichnungen von [1]. Es zeigt sich, daß das folgende einfache Lemma interessante Konsequenzen für vollsymmetrische Algebren hat, die z. B. eine Lücke im Beweis des Satzes III in [1], S. 315 (vgl. Satz 2) schließen.

Lemma. *R sei eine Banachsche Algebra mit Einselement e. R_1 sei eine abgeschlossene Unteralgebra von R mit $e \in R_1$. x sei ein Element aus R_1, das bezüglich R ein Spektrum besitzt, dessen Komplement zusammenhängend ist. Dann hat x bezüglich R_1 und R das gleiche Spektrum.*[1]).

Beweis. Das Spektrum von x bezüglich R ist eine Teilmenge des Spektrums von x bezüglich R_1, da $R \supset R_1$. $x = (x - \lambda e)^{-1}$ ist eine analytische Funktion von λ auf dem Komplement $\mathfrak{R}_x$ des Spektrums von x bezüglich R mit Werten aus R ([1], S. 184). Wir zeigen, daß für $\lambda \in \mathfrak{R}_x$ stets $x_\lambda \in R_1$ gilt. Dann ist das Spektrum von x bezüglich R und R_1 dasselbe. Ist f ein beschränktes, lineares Funktional über R, so ist mit x_λ auch $f(x_\lambda)$ eine analytische Funktion über $\mathfrak{R}_x$. Für $|\lambda| > |x|$ ($|x|$ = Norm von x) gilt

$$x_\lambda = (x - \lambda e)^{-1} = -\frac{1}{\lambda} e - \frac{1}{\lambda^2} x - \frac{1}{\lambda^3} x^2 - \cdots .$$

Wegen $x \in R_1$ ist $x_\lambda \in R_1$ für alle $|\lambda| > |x|$. Ist f ein beschränktes, lineares Funktional über R, das auf R_1 verschwindet, so ist $f(x_\lambda)$ eine analytische Funktion, die für $|\lambda| > |x|$ verschwindet. Da der Definitionsbereich dieser Funktion zusammenhängend ist, gilt $f(x_\lambda) = 0$ für alle $\lambda \in \mathfrak{R}_x$. Da $f(x_\lambda) = 0$ für alle linearen Funktionale über R gilt, die auf R_1 verschwinden, ist $x_\lambda \in R_1$ für alle $\lambda \in \mathfrak{R}_x$ (vgl. [1], S. 67).

Satz 1. *Es sei R eine vollsymmetrische Banachsche Algebra mit Einselement e und R_1 eine symmetrische abgeschlossene Unteralgebra von R mit $e \in R_1$. Dann ist auch R_1 vollsymmetrisch.*

Beweis. Wir haben zu zeigen, daß für jedes $x \in R_1$ $(x^*x + e)^{-1}$ existiert und zu R_1 gehört. Das Spektrum von x^*x bezüglich R liegt in der nichtnegativen reellen Achse ([1], S. 312). Wegen des Lemmas gilt dies dann auch für das Spektrum bezüglich R_1. Also gehört -1 nicht zum Spektrum von x^*x bezüglich R_1, d. h. $(x^*x + e)^{-1}$ existiert und gehört zu R_1.

Satz 2. *Unter den Voraussetzungen von Satz 1 läßt sich jedes positive, lineare Funktional über R_1 zu einem positiven, linearen Funktional über R fortsetzen.*

[1]) (Hinzugefügt bei der Korrektur am 27. 2. 61): Vgl. auch C. E. Rickart, Banach Algebras, New York 1960, S. 34 und S. 223.

Bemerkung. Das ist ein Teil des Satzes III in [1], S. 315. Im Beweis des Satzes befindet sich folgende Lücke. Beim Beweis wird der Satz von Krein ([1], S. 77) verwendet. Dabei wird benutzt, daß ein positives Funktional über R_1 auf $H_1 \cap P$ nur nichtnegative Werte annimmt. Dabei ist H_1 die Menge der hermitischen Elemente aus R_1 und P die Menge der hermitischen Elemente aus R mit nichtnegativem Spektrum bezüglich R, d. h. das Spektrum besteht nur aus Punkten $\lambda \geqq 0$. Es ist aber zunächst denkbar, daß es Elemente in H_1 gibt, die zwar ein nichtnegatives Spektrum bezüglich R besitzen, aber nicht bezüglich R_1 und auf denen ein positives Funktional über R_1 negative Werte annehmen kann. Das ist nach unserem Lemma nicht möglich, denn die Elemente aus $H_1 \cap P$ haben bezüglich R und R_1 dasselbe Spektrum.

Zwei weitere Bemerkungen scheinen nützlich zu sein, um den Beweis in [1], S. 315 zu vervollständigen: 1. Ein lineares Funktional über einer vollsymmetrischen Algebra R ist dann und nur dann positiv, wenn $f(x) \geqq 0$ für alle $x \in P$ gilt.

Beweis. Dann: $x^*x \in P$ nach [1], VI. S. 312, also ist $f(x^*x) \geqq 0$. Nur dann: Ist $x \in P^+$ ($P^+ =$ Menge der hermitischen Elemente aus R mit positivem Spektrum), so ist $x = y^*y$ für ein $y \in R$ ([1], VII. S. 312), also $f(x) = f(y^*y) \geqq 0$. Ist $x \in P$, so ist $x + \alpha e \in P^+$ für $\alpha > 0$. Also ist $f(x) + \alpha f(e) \geqq 0$. Für $\alpha \to 0$ folgt hieraus $f(x) \geqq 0$.

2. Der Satz von Krein ([1], S. 77) bleibt richtig, wenn man für den „positiven" Kegel K nur voraussetzt, daß aus $x \in K$, $y \in K$ und $\alpha \geqq 0$ folgt $\alpha x \in K$ und $x + y \in K$.

Im Zusammenhang mit dem Lemma ist folgender Satz von Interesse.

Satz 3. *Unter den Voraussetzungen von Satz 1 hat jedes Element $x \in R_1$ dasselbe Spektrum bezüglich R und R_1.*

Beweis. Das Spektrum von x bezüglich R ist im Spektrum von x bezüglich R_1 enthalten, da $R \supset R_1$. Es gilt auch die umgekehrte Inklusion. Es sei λ aus dem Spektrum von x bezüglich R_1. Dann existiert $(x - \lambda e)^{-1}$ in R_1 nicht. Also gibt es ein Linksideal I_1 in R_1 mit $I_1 \neq R_1$ und $x - \lambda e \in I_1$ (vgl. [1], S. 170). Nach [1], I. S. 313 gibt es ein positives, lineares Funktional über R_1 mit $f(e) = 1$ und $f(y^*y) = 0$ für $y \in I_1$. Nach Satz 2 kann dieses Funktional positiv auf R fortgesetzt werden. $\bar{f}$ sei diese Fortsetzung und $\bar{I}$ sei das Linksideal in R aller $y \in R$ mit $\bar{f}(y^*y) = 0$. Wegen $f(e) = 1$ ist $\bar{I} \neq R$ und wegen $f((x - \lambda e)^*(x - \lambda e)) = 0$ ist $x - \lambda e \in \bar{I}$. Also existiert $(x - \lambda e)^{-1}$ auch in R nicht, d. h. λ gehört auch zum Spektrum von x bezüglich R.

Korollar. *Unter den Voraussetzungen von Satz 1 gilt insbesondere: Ist $x \in R_1$ und existiert x^{-1} in R, so ist $x^{-1} \in R_1$.*

Beweis. x^{-1} existiert in R bzw. R_1 ist gleichwertig mit: 0 gehört nicht zum Spektrum von x bezüglich R bzw. R_1.

Literaturverzeichnis

[1] M. G. Neumark, Normierte Algebren. Berlin 1959.

Eingegangen am 16. 9. 1960

Anschrift der Autoren:

James M. G. Fell und Elmar Thoma
Department of Mathematics
University of Washington
Seattle 5 (Wash.), USA

Ordnungsfunktionen, die auf Seiteneinteilungen besonderer Art führen

Von

Erich Glock

Die von Sperner in [4], [5] eingeführten geometrischen Ordnungsfunktionen[1]) führen bekanntlich zu Seiteneinteilungen, d. h. sie bewirken bei jeder Hyperebene eine Einteilung der nicht mit ihr inzidierenden Punkte in (höchstens) zwei Klassen, ihre Seiten. Diese Seiteneinteilungen sind von sehr allgemeiner Art. Selbst dann, wenn man in affinen Räumen noch die Hyperebenenrelation[1]) fordert, brauchen sie nur wenige der Eigenschaften zu haben, die man aus der „klassischen Geometrie" gewohnt ist.

Es liegt daher nahe, in affinen Räumen nach solchen Ordnungsfunktionen zu fragen, deren zugehörige Seiteneinteilungen gewisse Eigenschaften haben, die man „naturgemäß" von ihnen erwartet. Sperner hat nun z. B. in [6] gezeigt, zu welchen Ordnungsfunktionen Seiteneinteilungen mit *konvexen* Seiten gehören. Das Ziel dieser Note soll sein, zu ermitteln, wann die beiden Seiten jeder Hyperebene *gleichmächtig* sind.

Während aber die hier angegebene Bedingung im allgemeinen Fall nur hinreichend ist (Abschnitt 2), wird sie sich bei vielen endlichen Geometrien — jedenfalls dann, wenn der Satz von Desargues gilt — auch als notwendig erweisen (Abschnitt 3).

1. Erklärungen. Wir legen unseren Untersuchungen einen *n-dimensionalen affinen Raum*[2]) zugrunde ($2 \leqq n < \infty$). Wenn nichts anderes gesagt wird, setzen wir bei $n = 2$ die Gültigkeit von keinerlei Schließungssätzen voraus. Punkte seien mit großen lateinischen, Hyperebenen (bei $n = 2$ Geraden) mit kleinen griechischen Buchstaben bezeichnet. PQ bedeute die Verbindungsgerade von P und Q. Inzidenz von P und ε bringen wir durch $P \in \varepsilon$ zum Ausdruck.

Unter einer *Ordnungsfunktion* [5, § 1] versteht man eine Abbildung o der Paare (ε, P) mit $P \notin \varepsilon$ in die Gruppe der Ordnung 2, deren Elemente mit $+1$ und -1 bezeichnet seien. Die Abbildung ζ, die durch $(P, \varepsilon, Q)^\zeta = (\varepsilon, P)^o\,(\varepsilon, Q)^o$ erklärt ist, heißt die *abgeleitete Ordnungsfunktion* [5, § 1] von o. Für sie gilt

$$(P, \varepsilon, Q)^\zeta\,(Q, \varepsilon, R)^\zeta = (P, \varepsilon, R)^\zeta\,. \tag{1}$$

Jede Abbildung ζ der Tripel (P, ε, Q) mit $P, Q \notin \varepsilon$ in die Gruppe der Ordnung 2 mit der Eigenschaft (1)[3]) ist eine abgeleitete Ordnungsfunktion. Man findet zu ihr eine

[1]) Diese Begriffe werden in Abschnitt 1 definiert.
[2]) Vgl. zu diesem Begriff etwa [3, Abschn. 1.2] für $n = 2$ und [2, I. § 2] für $n > 2$.
[3]) Aus (1) folgt auch $(P, \varepsilon, P)^\zeta = +1$, $(P, \varepsilon, Q)^\zeta = (Q, \varepsilon, P)^\zeta$.

Ordnungsfunktion o, deren Ableitung sie ist, indem man jeder Hyperebene ε einen nicht mit ihr inzidierenden Punkt P_ε zuordnet und $(\varepsilon, P)^o = (P_\varepsilon, \varepsilon, P)^\zeta$ setzt [5, § 1]. Auf diese Weise erhält man alle Ordnungsfunktionen bis auf diejenigen, die die Ableitung ζ_0 mit $(P, \varepsilon, Q)^{\zeta_0} = +1$ haben. Diese letzteren Ordnungsfunktionen haben die Form $(\varepsilon, P)^o = \varepsilon^\alpha$, wo α eine Abbildung der Menge aller Hyperebenen in die Gruppe der Ordnung 2 mit $\varepsilon^\alpha \neq +1$ ist. Zwei verschiedene Ordnungsfunktionen o_1 und o_2 liefern genau dann dieselbe abgeleitete Ordnungsfunktion, wenn es eine Abbildung α der eben genannten Art mit

$$(\varepsilon, P)^{o_1} = (\varepsilon, P)^{o_2} \cdot \varepsilon^\alpha$$

gibt.

Jede abgeleitete Ordnungsfunktion ζ liefert eine *Seiteneinteilung* gemäß der Festsetzung, daß zwei nicht mit ε inzidierende Punkte P, Q genau dann auf derselben Seite der Hyperebene ε liegen sollen, wenn

$$(P, \varepsilon, Q)^\zeta = +1$$

ist.

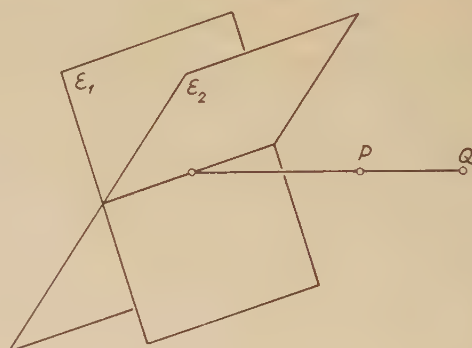
Besonderes Interesse finden diejenigen Seiteneinteilungen, die zu Ordnungsfunktionen gehören, die der *Hyperebenenrelation* (bei $n = 2$ *Geradenrelation*) [5, § 3] genügen. Diese lautet

$$(\varepsilon_1, P)^o (\varepsilon_1, Q)^o = (\varepsilon_2, P)^o (\varepsilon_2, Q)^o,$$

bzw. für abgeleitete Ordnungsfunktionen

(2) $$(P, \varepsilon_1, Q)^\zeta = (P, \varepsilon_2, Q)^\zeta,$$

wenn $PQ \cap (\varepsilon_1 \cap \varepsilon_2) \neq \varnothing$ und $P, Q \notin \varepsilon_i$ $(i = 1, 2)$.



Solche Seiteneinteilungen induzieren nämlich einen *Zwischen-Begriff* auf den Geraden des affinen Raumes [5, § 3].

Verabredung. Im folgenden werden wir uns nur noch mit abgeleiteten Ordnungsfunktionen, die zudem der Hyperebenenrelation genügen, befassen und diese daher kurz „*Ordnungsfunktionen*" nennen.

2. Hinreichende Bedingung für gleichmächtige Seiten. Zu einer Ordnungsfunktion ζ kann man eine Vielfalt von weiteren Ordnungsfunktionen ζ_ι durch den Ansatz

(3) $$(P, \varepsilon, Q)^{\zeta_\iota} = (P, \varepsilon, Q)^\zeta \cdot P^\iota Q^\iota$$

gewinnen, wo ι eine beliebige Abbildung der Menge aller Punkte in die Gruppe der Ordnung 2 bedeutet. Wenn ζ die Beziehungen (1) und (2) erfüllt, ist dies offenbar auch für ζ_ι der Fall.

Ist nun eine Hyperebene η gegeben, so läßt sich eine Abbildung ι so finden, daß ζ_ι für dieses η vorgeschriebene Werte annimmt, welche die Bedingung (1) (mit $\varepsilon = \eta$)

erfüllen. Man braucht ja nur einen festen Punkt O ($\notin \eta$) auszuwählen und $P^\iota = (O, \eta, P)^\zeta (O, \eta, P)^{\zeta\iota}$ zu setzen.

Sagt man von zwei Ordnungsfunktionen ζ_1, ζ_2, sie gehören zur selben *Klasse* [4]), wenn es eine Abbildung ι obiger Art mit $\zeta_2 = (\zeta_1)_\iota$ gibt, dann können wir folgenden Satz aussprechen.

Satz 1. *In jeder Klasse gibt es eine Ordnungsfunktion, welche für eine Hyperebene die nicht mit ihr inzidierenden Punkte auf vorgeschriebene Art auf deren beide Seiten verteilt.*

Auf Grund dieses Sachverhalts wird man fragen, wie eine Ordnungsfunktion beschaffen sein muß, damit die beiden Seiten *jeder* Hyperebene gleiche Mächtigkeit haben.

Eine hinreichende Bedingung dafür liefert folgender Satz.

Satz 2. *Genügt eine von ζ_0 verschiedene Ordnungsfunktion der Parallelenbedingung, dann sind bei der zugehörigen Seiteneinteilung die beiden Seiten jeder Hyperebene gleichmächtig.*

Die *Parallelenbedingung* [6, Seite 150] besagt

$$(P, \varepsilon, Q)^\zeta = +1, \text{ wenn } PQ \parallel \varepsilon. \tag{4}$$

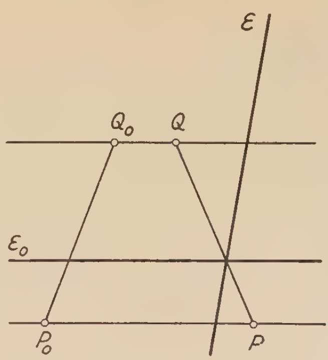
In jeder Klasse gibt es höchstens eine Ordnungsfunktion mit Parallelenbedingung, wie man aus (3) ohne weiteres ersieht. ζ_0 genügt trivialerweise der Parallelenbedingung; doch hat hier jede Hyperebene nur eine Seite.

Beweis von Satz 2. ζ sei eine Ordnungsfunktion der im Satz genannten Art.

I. Wegen $\zeta \neq \zeta_0$ gibt es ein Tripel $(P_0, \varepsilon_0, Q_0)$ mit

$$(P_0, \varepsilon_0, Q_0)^\zeta = -1. \tag{5}$$

Ist nun ε irgendeine Hyperebene $\nparallel \varepsilon_0$, dann ziehen wir durch einen Punkt von $\varepsilon_0 \cap \varepsilon$ eine Gerade, die weder in ε_0 noch in ε liegt und schneiden sie mit den zu ε_0 parallelen Hyperebenen durch P_0 und Q_0. Die Schnittpunkte seien P und Q. Dann gilt nach (4), falls $P_0 \neq P$, $Q_0 \neq Q$,



$$(Q_0, \varepsilon_0, Q)^\zeta = +1, \tag{6}$$

$$(P_0, \varepsilon_0, P)^\zeta = +1; \tag{7}$$

und diese Beziehungen gelten auch, falls $P_0 = P$ oder $Q_0 = Q$. Aus der Hyperebenenrelation (2) folgt weiter

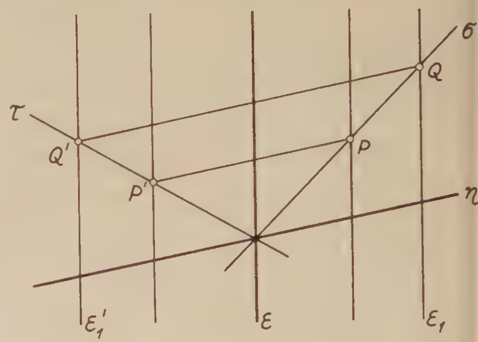
$$(P, \varepsilon_0, Q)^\zeta (P, \varepsilon, Q)^\zeta = +1. \tag{8}$$

Multiplikation der linken Seiten von (5), (6), (7), (8) ergibt $(P, \varepsilon, Q)^\zeta = -1$. — Für Hyperebenen $\parallel \varepsilon_0$ wiederholt man diesen Schluß (mit einer der eben betrachteten Hyperebenen ε an Stelle von ε_0) und erhält so das Ergebnis: Zu jeder Hyperebene ε gibt es Punkte P, Q mit $(P, \varepsilon, Q)^\zeta = -1$.

4) Gilt der Satz von Desargues, dann stimmt dieser Begriff der Klasse mit dem in [6] überein.

II. ε sei jetzt irgendeine Hyperebene. Ist $\varepsilon_1 \parallel \varepsilon$, dann liegen wegen (4) alle Punkte von ε_1 auf derselben Seite von ε. Damit ist es sinnvoll, von zwei zu ε parallelen Hyperebenen zu sagen, sie lägen auf derselben oder auf verschiedenen Seiten von ε. Zum Beweis des Satzes genügt es also, eine eineindeutige Abbildung der parallelen Hyperebenen der einen Seite auf die parallelen Hyperebenen der andern Seite von ε anzugeben. Zu diesem Zweck wählen wir zwei (nach I vorhandene) Punkte P, P' mit

(9) $$(P, \varepsilon, P')^{\zeta} = -1$$



und eine Hyperebene $\eta \parallel PP'$. σ bzw. τ seien die Hyperebenen des durch ε und η bestimmten Büschels, die P bzw. P' enthalten. Nun bilden wir die zu ε parallelen Hyperebenen mittels σ perspektiv auf die zu η parallelen Hyperebenen ab und darauf diese mittels τ perspektiv wieder auf die zu ε parallelen Hyperebenen. Bei dieser eineindeutigen Abbildung der zu ε parallelen Hyperebenen auf sich geht jede Hyperebene in eine solche der anderen Seite über. Denn wenn etwa $\varepsilon_1 \parallel \varepsilon$ und ε_1' das Bild von ε_1 bei dieser Abbildung ist, dann wählen wir Punkte Q bzw. Q' in $\varepsilon_1 \cap \sigma$ bzw. $\varepsilon_1' \cap \tau$ und finden dann nach (2) und (4)

$$\begin{aligned}
(P, \varepsilon, Q)^{\zeta} (P, \eta, Q)^{\zeta} &= +1,\\
(P', \varepsilon, Q')^{\zeta} (P', \eta, Q')^{\zeta} &= +1,\\
(P, \eta, P')^{\zeta} &= +1,\\
(Q, \eta, Q')^{\zeta} &= +1.
\end{aligned}$$

Multipliziert man die linken Seiten dieser Gleichungen miteinander und mit der von (9), so ergibt sich

$$(Q, \varepsilon, Q')^{\zeta} = -1,$$

d. h. ε_1 und ε_1' liegen auf verschiedenen Seiten von ε. — Damit ist der Beweis von Satz 2 vollendet.

Notwendig ist die in Satz 2 genannte Bedingung allerdings nicht, wie man an folgendem Beispiel sieht. Gegeben sei der reelle n-dimensionale Raum $R^{(n)}$ $(n \geqq 2)$. ζ sei die (einzige) Ordnungsfunktion $\neq \zeta_0$ mit Parallelenbedingung. Nach Einführung eines Parallelkoordinatensystems erkläre man ι durch $P^{\iota} = -1$, wenn alle n Koordinaten von P rational sind und $P^{\iota} = +1$ sonst. ζ_{ι} genügt dann nicht der Parallelenbedingung; dagegen haben alle Hyperebenen bei der zu ζ_{ι} gehörenden Seiteneinteilung gleichmächtige Seiten. — Durch eine leichte Abänderung dieses Beispiels erhält man ein solches, wo die Ordnungsfunktion zur Klasse von ζ_0 gehört. Man setze etwa $P^{\iota} = -1$, wenn die erste Koordinate von P rational ist und $P^{\iota} = +1$ sonst. Die durch $(P, \varepsilon, Q)^{\zeta_1} = P^{\iota} Q^{\iota}$ gegebene Ordnungsfunktion ζ_1 bewirkt dann ebenfalls, daß alle Hyperebenen gleichmächtige Seiten haben.

3. Endliche Geometrien. Unter der *Ordnung* N eines affinen Raumes mit endlich vielen Punkten versteht man die Anzahl der Punkte, die mit einer Geraden inzidieren. Ein Hyperebenenbüschel besteht dann aus $N + 1$ Elementen, und eine Schar paralleler Hyperebenen hat N Elemente.

Zunächst folgt mit Satz 2 aus der trivialen Feststellung, daß bei gerader Ordnung eine Hyperebene nicht gleich viele parallele Hyperebenen auf jeder ihrer Seiten haben kann, folgender Satz:

Satz 3. *Bei gerader Ordnung N gibt es keine von ζ_0 verschiedene Ordnungsfunktionen, die der Parallelenbedingung genügen*[5]).

Daß es bei geradem N überhaupt keine Seiteneinteilungen mit gleichmächtigen Seiten gibt, können wir lediglich als Vermutung vermerken[6]).

Versucht man bei einem endlichen affinen Raum Beispiele von der Art zu konstruieren, wie wir sie am Schluß von Abschnitt 2 für den $R^{(n)}$ gefunden haben, so gelingt dies nicht. Dies liegt an folgender Tatsache.

Satz 4. *Genügt in einem endlichen affinen Raum eine Ordnungsfunktion ζ der Parallelenbedingung, dann hat keine der übrigen in der Klasse von ζ liegenden Ordnungsfunktionen die Eigenschaft, daß die beiden Seiten jeder Hyperebene gleich viele Punkte enthalten.*

Beweis. I. $\zeta = \zeta_0$. Wir betrachten eine Schar von parallelen Hyperebenen ε_1, $\varepsilon_2, \ldots, \varepsilon_N$. Ist nun eine für alle Punkte erklärte Funktion ι gegeben, dann sei a_i die Anzahl der Punkte von ε_i mit $P^\iota = -1$ $(i = 1, \ldots, N)$. Wenn nun die zur Ordnungsfunktion $(\zeta_0)_\iota$ gehörende Seiteneinteilung doch die fragliche Eigenschaft hätte, dann müßten die Gleichungen

$$\sum_{i=1}^{j-1} a_i + \sum_{i=j+1}^{N} a_i = \frac{1}{2}(N-1)\,N^{n-1} \quad (j = 1, \ldots, N)$$

gelten. Dieses Gleichungssystem hat die Lösung

$$a_1 = a_2 = \cdots = a_N = \frac{1}{2}\,N^{n-1}$$

und nur diese[7]). Bei ungeradem N hat man hierin sofort einen Widerspruch, bei geradem N ergibt sich ein solcher unter Benutzung von folgendem Hilfssatz.

Hilfssatz. *In einem endlichen affinen Raum gibt es keine Punktmenge, die weder leer ist noch alle Punkte umfaßt und die mit jeder Hyperebene gleich viele Punkte gemein hat.*

II. $\zeta \neq \zeta_0$. Nach Satz 3 ist hier N ungerade. Zur Abkürzung setzen wir $\frac{1}{2}(N-1) = K$.

---

[5]) Wenn der Satz von Desargues gilt, dann ist dies ein bekanntes Ergebnis, weil dann nach [1] die Ordnungsfunktionen mit Parallelenbedingung in eineindeutigem Zusammenhang mit den sogenannten Halbordnungen des Koordinatenkörpers stehen und die Galoisfelder mit Charakteristik 2 nur die triviale Halbordnung besitzen.

[6]) Diese Vermutung wäre wegen Satz 4 z. B. dann bestätigt, wenn bei geradem N jede Ordnungsfunktion in der Klasse von ζ_0 läge.

[7]) Man stellt leicht fest, daß die Determinante dieses Gleichungssystems $= (-1)^{N-1}(N-1) \neq 0$ ist.

Wir fassen wieder eine Schar paralleler Hyperebenen $\varepsilon_1, \ldots, \varepsilon_N$ ins Auge und nach Vorgabe einer Funktion ι möge a_i wieder die Bedeutung wie eben haben. Dann mögen $\varepsilon_{i_1}, \ldots, \varepsilon_{i_K}$ bezüglich ζ auf der einen Seite und $\varepsilon_{i_1'}, \ldots, \varepsilon_{i_K'}$ auf der anderen Seite von ε_i liegen. $(i_1, \ldots, i_K, i, i_1', \ldots, i_K')$ entsteht also aus $(1, \ldots, N)$ durch eine Permutation. Wir wollen annehmen, daß die zur Ordnungsfunktion ζ_ι gehörige Seiteneinteilung die Eigenschaft hat, daß die beiden Seiten jeder Hyperebene gleich viele Punkte enthalten. Da ein Blick auf (3) lehrt, daß bei ζ_ι gegenüber ζ genau die Punkte P mit $P^\iota = -1$ die Seite gewechselt haben, müssen folgende Gleichungen gelten:

$$\sum_{k=1}^{K} a_{i_k} = \sum_{k=1}^{K} a_{i_k'} \qquad (i = 1, \ldots, N).$$

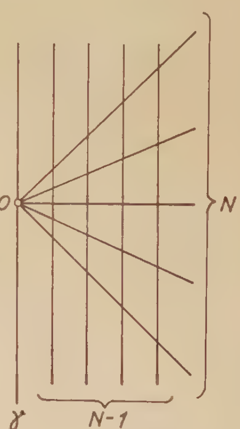
Dieses Gleichungssystem hat die Lösungen

$$a_1 = a_2 = \cdots = a_N$$

und nur diese[8]). Daher müssen überhaupt *alle* Hyperebenen des Raumes gleichviele Punkte mit $P^\iota = -1$ enthalten. Aus unserem Hilfssatz folgt dann, daß $a_i = 0$ oder $a_i = N^{n-1}$ sein muß, d. h. die Funktion ι ist eine Konstante und damit $\zeta_\iota = \zeta$.

Nun muß nur noch der Hilfssatz bewiesen werden. $\mathfrak{M}$ sei eine nichtleere Punktmenge derart, daß jede Hyperebene genau k Punkte aus $\mathfrak{M}$ enthält.

I. $n = 2$. O sei ein Punkt von $\mathfrak{M}$. Wir betrachten eine mit O inzidierende Gerade γ sowie die durch γ bestimmte Parallelenschar und das durch O bestimmte Geradenbüschel. Die $N - 1$ von γ verschiedenen Geraden der Parallelenschar enthalten zusammen $(N - 1) \cdot k$ Punkte von $\mathfrak{M}$. Die N von γ verschiedenen Geraden des Büschels enthalten zusammen $N \cdot (k - 1)$ von O verschiedene Punkte von $\mathfrak{M}$. Es muß also die Identität



$$(N - 1) \cdot k = N \cdot (k - 1)$$

gelten, d. h. es ist nur $k = N$ möglich, w. z. b. w.

II. $n > 2$. Annahme: Der Hilfssatz sei für Räume mit Dimension $< n$ schon bewiesen. — Wir betrachten erstens eine Schar paralleler Hyperebenen — eine davon heiße ε — und zweitens ein ε enthaltendes Hyperebenenbüschel — sein Träger sei die Hypergerade[9]) η —. Die $N - 1$ von ε verschiedenen Hyperebenen der Parallelenschar enthalten zusammen $(N - 1) \cdot k$ Punkte von $\mathfrak{M}$. Wenn genau k_0 Punkte von $\mathfrak{M}$ in η liegen, dann enthalten die von ε verschiedenen N Hyperebenen des Büschels zu-

[8]) In der Matrix des Gleichungssystems stehen in der Hauptdiagonale lauter Nullen und außerhalb derselben nur die Zahlen 1 und -1. Diese Matrix hat den Rang $N - 1$, da die aus den ersten $N - 1$ Zeilen und Spalten gebildete Unterdeterminante nicht verschwindet. Das erkennt man mit Hilfe des Ergebnisses von Fußnote [7]), wenn man die Unterdeterminante modulo 2 berechnet.

[9]) Das ist ein $(n - 2)$-dimensionaler linearer Unterraum, bei $n = 3$ eine Gerade.

sammen $N \cdot (k - k_0)$ Punkte von $\mathfrak{M}$, die nicht zugleich in η liegen. Es muß nun

$$(N-1) \cdot k = N \cdot (k - k_0)$$

gelten. Also ist $k_0 = k/N$. Da man diese Betrachtung für jedes ε enthaltende Büschel durchführen kann, enthalten alle in ε liegenden Hypergeraden k/N Punkte von $\mathfrak{M}$. Das ist aber nach Induktionsvoraussetzung nur möglich, wenn $k_0 = N^{n-1}$, d. h. wenn $k = N^n$ ist, w. z. b. w.

Satz 4 gestattet nun in gewissen Fällen, Satz 2 umzukehren. Es gilt nämlich folgender Satz:

Satz 5. *Enthält bei einem endlichen affinen Raum jede Klasse von Ordnungsfunktionen eine solche, die der Parallelenbedingung genügt, dann haben genau die zu den von* ζ_0 *verschiedenen Ordnungsfunktionen mit Parallelenbedingung gehörenden Seiteneinteilungen die Eigenschaft, daß die beiden Seiten jeder Hyperebene gleich viele Punkte enthalten.*

Die in Satz 5 genannte Voraussetzung ist insbesondere dann erfüllt, wenn der Satz von Desargues gilt — also immer bei $n > 2$ —, weil man dann nach [6, Seite 152] zu jeder Ordnungsfunktion eine andere Ordnungsfunktion konstruieren kann, die der Parallelenbedingung genügt und derselben Klasse angehört.

Literaturverzeichnis

[1] F. Bachmann und W. Klingerberg, Über Seiteneinteilungen in affinen und euklidischen Ebenen. Math. Ann. **123**, 288—301 (1951).
[2] H. Lenz, Zur Begründung der analytischen Geometrie. S-Ber. Bayer. Akad. Wiss., math.-naturw. Kl. 17—72 (1954).
[3] G. Pickert, Projektive Ebenen. Springer, Berlin-Göttingen-Heidelberg 1955.
[4] E. Sperner, Die Ordnungsfunktionen einer Geometrie. Arch. Math. **1**, 9—12 (1948/49).
[5] E. Sperner, Die Ordnungsfunktionen einer Geometrie. Math. Ann. **121**, 107—130 (1949).
[6] E. Sperner, Konvexität bei Ordnungsfunktionen. Abh. math. Sem. Univ. Hamburg **16**, 140 bis 154 (1949).

Eingegangen am 17. 8. 1960

Anschrift des Autors:
Erich Glock
Mathematisches Institut
der Technischen Hochschule
Stuttgart

Eine Bemerkung über Lagerungen konvexer Kegel

Von

Helmut Groemer

Eine Menge $\{K_i\}$ von konvexen Körpern K_i des euklidischen n-dimensionalen Raumes heiße eine Lagerung, wenn je zwei K_i translationsgleich sind und höchstens Randpunkte gemeinsam haben. Im folgenden Satz soll für die Dichte einer Lagerung konvexer Kegel eine nur von der Dimension n abhängige obere Schranke angegeben werden. Es sei immer vorausgesetzt, daß die Dichte existiere.

Satz. *Für die Dichte d einer Lagerung konvexer Kegel gilt*

$$d \leqq \frac{1}{2} \frac{2^n}{2^n - 1}. \tag{1}$$

Die Abschätzung (1) läßt sich für $n = 2$ nicht verbessern. Für große n hingegen dürfte noch eine wesentliche Verschärfung möglich sein. Mit dem hier angewandten Beweisverfahren gelingt eine Verbesserung von (1) nur dann, wenn spezielle Voraussetzungen über die Basis der Kegel vorliegen. Zum Beispiel gilt für eine Lagerung von Simplices (C. A. Rogers und G. C. Shephard [1])

$$d \leqq 2^n \binom{2n}{n}^{-1} \tag{2}$$

oder für den Fall, daß eine Lagerung von Kegeln vorliegt, deren Basis eine $(n-1)$-dimensionale Kugel ist,

$$d \leqq \frac{\pi}{\sqrt{14}} \left(\sqrt{2} + 1\right) = 0{,}5417\ldots \qquad (n = 3) \tag{3}$$

und

$$d \leqq (n+1) \frac{2^{n-1}}{2^n - 1} \left(\frac{3}{\sqrt{17}}\right)^{n+1} \qquad (n > 3). \tag{4}$$

Es soll nun der Beweis des obigen Satzes gegeben werden. Bezeichnet K einen konvexen Körper, so soll K^* den durch Zentralsymmetrisierung aus K hervorgehenden symmetrischen konvexen Körper bedeuten (vgl. Bonnesen-Fenchel [2]). $V(K)$ sei das Volumen von K. Ist $\{K_i\}$ eine Lagerung und bedeuten K_i^+ diejenigen symmetrischen konvexen Körper, die aus K_1 durch dieselben Translationen hervorgehen, welche K_1 in K_i überführen, so ist auch $\{K_i^+\}$ eine Lagerung. Diese Tatsache wurde im wesentlichen bereits von H. Minkowski [3] bewiesen; auch in [4] oder [5] kann man dafür einen Beweis finden. S_r bedeute eine n-dimensionale Kugel mit dem Radius r und dem Mittelpunkt im Koordinatenursprung. Ist n_r die Anzahl der K_i mit $K_i \subset S_r$,

so werde die Dichte d von K_i wie üblich durch

$$d = \lim_{r \to \infty} \frac{n_r V(K_i)}{V(S_r)}$$

erklärt. Definiert man n_r^+ und d^+ analog wie n_r und d, jedoch für K_i^+ anstatt K_i, so ist offenbar für $r \to \infty$

$$n_r = n_r^+ + o(V(S_r))$$

und man erhält die von C. A. Rogers und G. C. Shephard [1] angegebene Beziehung

$$d = \lim_{r \to \infty} \frac{n_r V(K_i)}{V(S_r)} = \frac{V(K_i)}{V(K_i^+)} \lim_{r \to \infty} \frac{n_r^+ V(K_i^+)}{V(S_r)} = \frac{V(K_i)}{V(K_i^+)} d^+ . \tag{5}$$

Aus (5) folgt sofort die Richtigkeit von (1), sobald für einen beliebigen konvexen Kegel K

$$V(K^*) \geqq V(K) \frac{2^n - 1}{2^{n-1}} \tag{6}$$

gezeigt ist. Man darf offenbar voraussetzen, daß K die Höhe 2 hat. B sei die Basis von K, und H bedeute die Ebene, die B enthält. $H(x)$ sei eine zu H parallele Ebene, die von H den Abstand x hat; dabei sollen alle $H(x)$ und B auf ein und derselben Seite von H liegen. Aus der Definition von K^* entnimmt man, daß

$$V(H(0) \cap K^*) = V(B^*) \tag{7}$$

und

$$V(H(1) \cap K^*) = \frac{1}{2^{n-1}} V(B) \tag{8}$$

ist. Außerdem gilt stets (vgl. [1])

$$V(B) \leqq V(B^*) \tag{9}$$

und da K ein Kegel ist

$$V(K) = \frac{2}{n} V(B) . \tag{10}$$

Aus (7), (8), (9), (10) und der Symmetrie von K^* erhält man mittels der Brunn-Minkowskischen Ungleichung

$$V(K) = 2 \int_0^1 V(H(x) \cap K^*) \, dx \geqq 2 \int_0^1 \left(\left((1-x) \frac{1}{2^{n-1}} V(B) \right)^{\frac{1}{n-1}} + x V(B)^{\frac{1}{n-1}} \right)^{n-1} dx =$$

$$= \frac{2}{n} V(B) \frac{2^n - 1}{2^{n-1}} = V(K) \frac{2^n - 1}{2^{n-1}} .$$

Damit ist (6) bewiesen. Für $n = 3$ wurde (6) bereits von Th. Estermann [6] bewiesen.

Es sind noch die Ungleichungen (3) und (4) zu beweisen. Ist K ein Kegel, dessen Basis eine Kugel vom Radius r ist, so hat K^* die Eigenschaft, daß jeder Schnitt mit einer Ebene E, die parallel zur Basis ist, eine $(n-1)$-dimensionale Kugel ergibt, deren Radius zwischen $\frac{1}{2} r$ und r liegt. Für die Dichte d_0 der Lagerung aller dieser Kugeln in E gilt nach R. A. Rankin [7]

$$(11) \qquad d_0 \leqq (n+1)\left(\frac{3}{\sqrt{17}}\right)^{n+1}$$

und nach L. Fejes Tòth [8] ($n = 3$)

$$(12) \qquad d_0 \leqq \frac{\pi}{8}\left(\sqrt{2}+1\right).$$

Da dies für jede Ebene E, die parallel zu den Basen der Kegel ist, gilt, folgt $d^+ \leqq d_0$ und damit erhält man (3), (4) aus (5), (11) und (12).

Es gibt noch einige andere Klassen konvexer Körper, für deren Lagerungsdichten man aus (5) Abschätzungen erhält. Zum Beispiel ergeben sich aus bekannten Abschätzungen der Dichten von Kugellagerungen entsprechende Aussagen über konvexe Körper konstanter Breite. Auch bei E. Hlawka [9] wird (5) bewiesen und angewendet.

Literaturverzeichnis

[1] C. A. Rogers and G. C. Shephard, The difference body of a convex body. Arch. Math. 8, 220—233 (1957).

[2] T. Bonnesen und W. Fenchel, Theorie der konvexen Körper. Ergebn. der Math. Bd. 3, Berlin 1934.

[3] H. Minkowski, Dichteste gitterförmige Lagerung kongruenter Körper. Ges. Abh. Bd. 2, 1—42, Leipzig u. Berlin 1911.

[4] H. Groemer, Abschätzungen für die Anzahl der konvexen Körper, die einen konvexen Körper berühren. Monatsh. Math. 65, 74—81 (1961).

[5] H. Hadwiger, Über Treffanzahlen bei translationsgleichen Eikörpern. Arch. Math. 8, 212 bis 213 (1957).

[6] Th. Estermann, Über den Vektorenbereich eines konvexen Körpers. Math. Z. 28, 471 bis 475 (1928).

[7] R. A. Rankin, On the closest packing of spheres in n dimensions. Ann. of Math. 48, 1062 —1081 (1947).

[8] L. Fejes Toth, Lagerungen in der Ebene, auf der Kugel und im Raum. Berlin 1953.

[9] E. Hlawka, Ausfüllung und Überdeckung konvexer Körper durch konvexe Körper. Monatsh. Math. 53, 81—131 (1949).

Eingegangen am 8. 8. 1960

Anschrift des Autors:
Helmut Groemer
Department of Mathematics
Oregon State University
Corvallis (Ore.), USA